Module MA3412: Integral Domains, Modules and Algebraic Integers
Section 1
Hilary Term 2014

D. R. Wilkins

Contents

1 Commutative Rings and Polynomials

1.1 Rings

Definition A *ring* consists of a set R on which are defined operations of *addition* and *multiplication* satisfying the following axioms:

- $x+y = y+x$ for all elements x and y of R (i.e., addition is *commutative*);
- $(x+y)+z = x+(y+z)$ for all elements x, y and z of R (i.e., addition is *associative*);
- there exists an an element 0_R of R (known as the *zero element* of the ring R) with the property that $x + 0_R = x$ for all elements x of R;
- given any element x of R, there exists an element $-x$ of R with the property that $x + (-x) = 0_R$;
- $x(yz) = (xy)z$ for all elements x, y and z of R (i.e., multiplication is *associative*);
- $x(y+z) = xy + xz$ and $(x+y)z = xz + yz$ for all elements x, y and z of R (the *Distributive Law*).

Lemma 1.1 *Let R be a ring. Then $x0_R = 0_R$ and $0_Rx = 0_R$ for all elements x of R.*

Proof The zero element 0_R of the ring R satisfies $0_R + 0_R = 0_R$. It follows from the Distributive Law that

$$x0_R + x0_R = x(0_R + 0_R) = x0_R.$$

On adding $-(x0_R)$ to both sides of this identity we see that $x0_R = 0_R$. Also

$$0_Rx + 0_Rx = (0_R + 0_R)x = 0_Rx,$$

and therefore $0_Rx = 0_R$. ∎

Lemma 1.2 *Let R be a ring. Then $(-x)y = -(xy)$ and $x(-y) = -(xy)$ for all elements x and y of R.*

Proof It follows from the Distributive Law that

$$xy + (-x)y = (x + (-x))y = 0_Ry = 0_R$$

and

$$xy + x(-y) = x(y + (-y)) = x0_R = 0_R.$$

Therefore $(-x)y = -(xy)$ and $x(-y) = -(xy)$. ∎

Definition A subset S of a ring R is said to be a *subring* of R if $0_R \in S$, $a + b \in S$, $-a \in S$ and $ab \in S$ for all $a, b \in S$.

Definition A ring R is said to be *commutative* if $xy = yx$ for all $x, y \in R$.

Definition A ring R is said to be *unital* if it possesses a non-zero multiplicative identity element 1_R with the property that $1_R x = x = x 1_R$ for all $x \in R$.

Example Let n be a positive integer. Then the set of all $n \times n$ matrices with real coefficients, with the usual operations of matrix addition and matrix multiplication, is a ring. This ring is a unital ring: the multiplicative identity element is the identity $n \times n$ matrix. The ring of $n \times n$ matrices with real coefficients is a non-commutative ring when $n > 1$.

1.2 Integral Domains and Fields

Definition A unital commutative ring R is said to be an *integral domain* if the product of any two non-zero elements of R is itself non-zero.

Definition A *field* consists of a set K on which are defined operations of *addition* and *multiplication* satisfying the following axioms:

- $x+y = y+x$ for all elements x and y of K (i.e., addition is *commutative*);
- $(x + y) + z = x + (y + z)$ for all elements x, y and z of K (i.e., addition is *associative*);
- there exists an an element 0_K of K (known as the *zero element* of the field K) with the property that $x + 0_K = x$ for all elements x of K;
- given any element x of K, there exists an element $-x$ of K with the property that $x + (-x) = 0_K$;
- $xy = yx$ for all elements x and y of K (i.e., multiplication is *commutative*);
- $x(yz) = (xy)z$ for all elements x, y and z of K (i.e., multiplication is *associative*);
- there exists a non-zero element 1_K of K (the *multiplicative identity element* of K) with the property that $1_K x = x$ for all elements x of K;
- given any non-zero element x of K, there exists an element x^{-1} of K with the property that $xx^{-1} = 1_K$;

- $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$ for all elements x, y and z of K (the *Distributive Law*).

An examination of the relevant definitions shows that a unital commutative ring R is a field if and only if, given any non-zero element x of R, there exists an element x^{-1} of R such that $xx^{-1} = 1_R$. Moreover a ring R is a field if and only if the set of non-zero elements of R is an Abelian group with respect to the operation of multiplication.

Lemma 1.3 *A field is an integral domain.*

Proof A field is a unital commutative ring. Let x and y be non-zero elements of a field K. Then there exist elements x^{-1} and y^{-1} of K such that $xx^{-1} = 1_K$ and $yy^{-1} = 1_K$. Then $xyy^{-1}x^{-1} = 1_K$. Now if it were the case that $xy = 0_K$ then it would follow that

$$1_K = (xy)(y^{-1}x^{-1}) = 0_K(y^{-1}x^{-1}) = 0_K$$

(see Lemma 1.1). But the definition of a field requires that $1_K \neq 0_K$. We conclude therefore that xy must be a non-zero element of the field K. ∎

The set $\mathbb{Z}$ of integers is an integral domain with respect to the usual operations of addition and multiplication. But $\mathbb{Z}$ is not a field. The sets $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ of rational, real and complex numbers are fields, and are thus integral domains.

1.3 Ideals

Definition Let R be a ring, and let 0_R denote the zero element of R. A subset I of R is said to be an *ideal* of R if $0_R \in I$, $a + b \in I$, $-a \in I$, $ra \in I$ and $ar \in I$ for all $a, b \in I$ and $r \in R$.

Definition An ideal I of R is said to be a *proper ideal* of R if $I \neq R$.

Note that an ideal I of a unital ring R is proper if and only if $1_R \notin I$, where 1_R denotes the multiplicative identity element of the ring R. Indeed if $1_R \in I$ then $r \in I$ for all $r \in R$, since $r = r1_R$.

Lemma 1.4 *A unital commutative ring R is a field if and only if the only ideals of R are the zero ideal $\{0_R\}$ and the ring R itself.*

Proof Suppose that R is a field. Let I be a non-zero ideal of R. Then there exists $x \in I$ satisfying $x \neq 0_R$. Moreover there exists $x^{-1} \in R$ satisfying $xx^{-1} = 1_R = x^{-1}x$. Therefore $1_R \in I$, and hence $I = R$. Thus the only ideals of R are $\{0_R\}$ and R.

Conversely, suppose that R is a unital commutative ring with the property that the only ideals of R are $\{0_R\}$ and R. Let x be a non-zero element of R, and let Rx denote the subset of R consisting of all elements of R that are of the form rx for some $r \in R$. It is easy to verify that Rx is an ideal of R. (In order to show that $yr \in Rx$ for all $y \in Rx$ and $r \in R$, one must use the fact that the ring R is commutative.) Moreover $Rx \neq \{0_R\}$, since $x \in Rx$. We deduce that $Rx = R$. Therefore $1_R \in Rx$, and hence there exists some element x^{-1} of R satisfying $x^{-1}x = 1_R$. This shows that R is a field, as required. ∎

The intersection of any collection of ideals of a ring R is itself an ideal of R. For if a and b are elements of R that belong to all the ideals in the collection, then the same is true of 0_R, $a + b$, $-a$, ra and ar for all $r \in R$.

Definition Let X be a subset of the ring R. The ideal of R *generated* by X is defined to be the intersection of all the ideals of R that contain the set X. Note that this ideal is well-defined and is the smallest ideal of R containing the set X (i.e., it is contained in every other ideal that contains the set X).

Any finite subset $\{f_1, f_2, \ldots, f_k\}$ of a ring R generates an ideal of R which we denote by $(f_1, f_2, \ldots, f_k)$.

Definition An ideal I of the ring R is said to be *finitely generated* if there exists a finite subset of R which generates the ideal I.

Lemma 1.5 *Let R be a unital commutative ring, and let X be a subset of R. Then the ideal generated by X coincides with the set of all elements of R that can be expressed as a finite sum of the form*

$$r_1x_1 + r_2x_2 + \cdots + r_kx_k,$$

where $x_1, x_2, \ldots, x_k \in X$ and $r_1, r_2, \ldots, r_k \in R$.

Proof Let I be the subset of R consisting of all these finite sums. If J is any ideal of R which contains the set X then J must contain each of these finite sums, and thus $I \subset J$. Let a and b be elements of I. It follows immediately from the definition of I that $0_R \in I$, $a + b \in I$, $-a \in I$, and $ra \in I$ for all $r \in R$. Also $ar = ra$, since R is commutative, and thus $ar \in I$. Thus I is an ideal of R. Moreover $X \subset I$, since the ring R is unital and $x = 1_Rx$ for all $x \in X$ (where 1_R denotes the multiplicative identity element of the ring R). Thus I is the smallest ideal of R containing the set X, as required. ∎

Each integer n generates an ideal $n\mathbb{Z}$ of the ring $\mathbb{Z}$ of integers. This ideal consists of those integers that are divisible by n.

Theorem 1.6 *Every ideal of the ring $\mathbb{Z}$ of integers is generated by some non-negative integer n.*

Proof The zero ideal is of the required form with $n = 0$. Let I be some non-zero ideal of $\mathbb{Z}$. Then I contains at least one strictly positive integer (since $-m \in I$ for all $m \in I$). Let n be the smallest strictly positive integer belonging to I. If $j \in I$ then we can write $j = qn + r$ for some integers q and r with $0 \le r < n$. Now $r \in I$, since $r = j - qn$, $j \in I$ and $qn \in I$. But $0 \le r < n$, and n is by definition the smallest strictly positive integer belonging to I. We conclude therefore that $r = 0$, and thus $j = qn$. This shows that $I = n\mathbb{Z}$, as required. ∎

1.4 Quotient Rings and Homomorphisms

Definition Let R be a ring and let I be an ideal of R. The *cosets* of I in R are the subsets of R that are of the form $I + x$ for some $x \in R$, where

$$I + x = \{a + x : a \in I\}.$$

We denote by R/I the set of cosets of I in R.

Let x and x' be elements of R. Then $I+x = I+x'$ if and only if $x-x' \in I$. Indeed if $I + x = I + x'$, then $x = c + x'$ for some $c \in I$. But then $x - x' = c$, and thus $x - x' \in I$. Conversely if $x - x' \in I$ then $x - x' = c$ for some $c \in I$. But then

$$I + x = \{a + x : a \in I\} = \{a + c + x' : a \in I\} = \{b + x' : b \in I\} = I + x'.$$

If x, x', y and y' are elements of R satisfying

$$I + x = I + x' \quad \text{and} \quad I + y = I + y'$$

then

$$\begin{aligned} (x + y) - (x' + y') &= (x - x') + (y - y'), \\ xy - x'y' &= xy - xy' + xy' - x'y' = x(y - y') + (x - x')y'. \end{aligned}$$

But $x - x' \in I$ and $y - y' \in I$, and therefore $x(y - y') \in I$ and $(x - x')y' \in I$, because I is an ideal. It follows that $(x + y) - (x' + y') \in I$ and $xy - x'y' \in I$, and therefore

$$I + x + y = I + x' + y' \quad \text{and} \quad I + xy = I + x'y'.$$

This shows that the quotient group R/I admits well-defined operations of addition and multiplication, defined such that

$$(I + x) + (I + y) = I + x + y \quad \text{and} \quad (I + x)(I + y) = I + xy$$

for all $x, y \in R$. One can readily verify that R/I is a ring with respect to these operations.

Definition Let R be a ring, and let I be an ideal of R. The *quotient ring* R/I corresponding to the ideal I of R is the set of cosets of I in R, where the operations of addition and multiplication of cosets are defined such that

$$(I + x) + (I + y) = I + x + y \quad \text{and} \quad (I + x)(I + y) = I + xy$$

for all $x, y \in R$.

Example Let n be an integer satisfying $n > 1$. The quotient $\mathbb{Z}/n\mathbb{Z}$ of the ring $\mathbb{Z}$ of integers by the ideal $n\mathbb{Z}$ generated by n is the ring of congruence classes of integers modulo n. This ring has n elements, and is a field if and only if n is a prime number.

Definition A function $\varphi: R \to S$ from a ring R to a ring S is said to be a *homomorphism* (or *ring homomorphism*) if and only if

$$\varphi(x + y) = \varphi(x) + \varphi(y) \quad \text{and} \quad \varphi(xy) = \varphi(x)\varphi(y)$$

for all $x, y \in R$. If in addition the rings R and S are unital then a homomorphism $\varphi: R \to S$ is said to be *unital* if $\varphi(1_R) = 1_S$, where 1_R and 1_S denote the multiplicative identity elements of the rings R and S respectively.

Let R and S be rings with zero elements 0_R and 0_S respectively, and let $\varphi: R \to S$ be a homomorphism from R to S. Let $x \in R$. Then

$$\varphi(x) = \varphi(x + 0_R) = \varphi(x) + \varphi(0_R).$$

It follows that $\varphi(0_R) = 0_S$. Also

$$\varphi(x) + \varphi(-x) = \varphi(x + (-x)) = \varphi(0_R) = 0_S,$$

and therefore $\varphi(-x) = -\varphi(x)$.

Definition Let R and S be rings, and let $\varphi: R \to S$ be a ring homomorphism. The *kernel* $\ker\varphi$ of the homomorphism φ is the ideal of R defined such that

$$\ker\varphi = \{x \in R : \varphi(x) = 0_S\}.$$

The image $\varphi(R)$ of the homomorphism is a subring of S; however it is not in general an ideal of S.

An ideal I of a ring R is the kernel of the quotient homomorphism that sends $x \in R$ to the coset $I + x$.

Definition An isomorphism $\varphi\colon R \to S$ between rings R and S is a homomorphism that is also a bijection between R and S. The inverse of an isomorphism is itself an isomorphism. Two rings are said to be *isomorphic* if there is an isomorphism between them.

Proposition 1.7 *Let R and S be rings, and let $\varphi\colon R \to S$ be a homomorphism from R to S. Then $\varphi(R) \cong R/\ker\varphi$, where $\ker\varphi$ denotes the kernel of the homomorphism φ.*

Proof Let x and y be elements of R, let 0_R and 0_S denote the zero elements of R and S respectively, and let $I = \ker\varphi$. Then

$$\begin{aligned} \varphi(x) = \varphi(y) \quad &\iff \quad \varphi(x) - \varphi(y) = 0_S \iff \varphi(x - y) = 0_S \\ &\iff \quad x - y \in I \iff I + x = I + y. \end{aligned}$$

It follows that there is a well-defined bijection $\tilde{\varphi}\colon R/I \to \varphi(R)$ defined such that $\tilde{\varphi}(I + x) = \varphi(x)$ for all $x \in R$. Moreover

$$\tilde{\varphi}((I + x) + (I + y)) = \tilde{\varphi}(I + x + y) = \varphi(x + y) = \varphi(x) + \varphi(y)$$

and

$$\tilde{\varphi}((I + x)(I + y)) = \tilde{\varphi}(I + xy) = \varphi(xy) = \varphi(x)\varphi(y)$$

for all $x, y \in R$. It follows that $\tilde{\varphi}\colon R/I \to \varphi(R)$ is an isomorphism, as required. ∎

1.5 The Characteristic of a Ring

Let R be a ring, and let $r \in R$. We may define $n.r$ for all natural numbers n by recursion on n so that $1.r = r$ and $n.r = (n - 1).r + r$ for all $n > 0$. We define also $0.r = 0_R$ and $(-n).r = -(n.r)$ for all natural numbers n. Then

$$(m + n).r = m.r + n.r, \qquad n.(r + s) = n.r + n.s,$$

$$(mn).r = m.(n.r), \qquad (m.r)(n.s) = (mn).(rs)$$

for all integers m an n and for all elements r and s of R.

In particular, suppose that R is a unital ring. Then the set of all integers n satisfying $n.1_R = 0_R$ is an ideal of $\mathbb{Z}$. Therefore there exists a unique non-negative integer p such that $p\mathbb{Z} = \{n \in \mathbb{Z} : n.1_R = 0_R\}$ (see Theorem 1.6). This integer p is referred to as the *characteristic* of the ring R, and is denoted by $\operatorname{char} R$.

Lemma 1.8 *Let R be an integral domain. Then either* $\operatorname{char} R = 0$ *or else* $\operatorname{char} R$ *is a prime number.*

Proof Let $p = \operatorname{char} R$. Clearly $p \neq 1$. Suppose that $p > 1$ and $p = jk$, where j and k are positive integers. Then $(j.1_R)(k.1_R) = (jk).1_R = p.1_R = 0_R$. But R is an integral domain. Therefore either $j.1_R = 0_R$, or $k.1_R = 0_R$. But if $j.1_R = 0_R$ then p divides j and therefore $j = p$. Similarly if $k.1_R = 0_R$ then $k = p$. It follows that p is a prime number, as required. ∎

1.6 Polynomial Rings

Let R be a unital commutative ring, let 0_R denote the zero element of R, and let $R[x]$ denote the set of all polynomials of the form

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where the coefficients $a_0, \ldots, a_n$ all belong to the ring R.

Each polynomial $f(x)$ with coefficients in the ring R determines and is determined by an infinite sequence

$$a_0, a_1, a_2, a_3, a_4, \ldots,$$

of elements of the ring R, where $a_j \in R$ for all non-negative integers j and $a_j \neq 0_R$ for at most finitely many values of j. The members of this infinite sequence are the *coefficients* of the polynomial $f(x)$. Given any polynomial $f(x)$ with coefficients $a_0, a_1, a_2, \ldots$, there exists some non-negative integer n such that $a_j = 0_R$ when $j > n$. The polynomial $f(x)$ is then represented by the expression

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n.$$

The polynomial $f(x)$ is said to be *non-zero* if $a_j \neq 0_R$ for at least one non-negative integer j. If the polynomial $f(x)$ is non-zero then there will be a well-defined non-negative integer d which is equal to the largest integer j for which $a_j \neq 0_R$. This non-negative integer d is the *degree* of the non-zero polynomial $f(x)$. A non-zero polynomial $f(x)$ of degree d with coefficients in the ring R is then uniquely representable in the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d,$$

where $a_0, a_1, \ldots, a_d \in R$ and $a_d \neq 0_R$. The coefficient a_d of f of degree d is referred to as the *leading coefficient* of the polynomial f.

Definition A non-zero polynomial $f(x)$ of degree d with coefficients in a unital commutative ring R is said to be *monic* if $a_d = 1_R$, where 1_R denotes the multiplicative identity element of the ring R, in which case the polynomial f can be represented in the form

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{d-1} x^{d-1} + x^d.$$

where $a_0, a_1, \ldots, a_{d-1} \in R$.

There are operations of addition and multiplication, defined on the set $R[x]$ of polynomials with coefficients in a unital commutative ring R. These operations are defined so as to generalize the standard operations of addition and multiplication defined on the set of polynomials with complex coefficients. Thus if

$$\begin{aligned} f(x) &= \sum_{n=0}^{r} b_n x^n = b_0 + b_1 x + b_2 x^2 + \cdots + b_{m-1} x^{m-1} + b_r x^r \\ g(x) &= \sum_{n=0}^{s} c_n x^n = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} + c_s x^s \end{aligned}$$

then

$$f(x) + g(x) = \sum_{n=0}^{s} g_n x^n = g_0 + g_1 x + g_2 x^2 + \cdots + g_{d-1} x^{d-1} + g_d x^d,$$

where $d = \max(r, s)$ and

$$g_j = \begin{cases} b_j + c_j & \text{if } 0 \le j \le \min(r, s); \\ b_j & \text{if } s < j \le r; \\ c_j & \text{if } r < j \le s. \end{cases}$$

Also

$$\begin{aligned} f(x)g(x) &= \sum_{j=0}^{r} \sum_{k=0}^{s} b_j c_k x^{j+k} \\ &= b_0 c_0 + (b_0 c_1 + b_1 c_0) x + (b_0 c_2 + b_1 c_1 + b_2 c_0) x^2 + \cdots \\ &\qquad + (b_{r-1} c_s + b_r c_{s-1}) x^{r+s-1} + b_r c_s x^{r+s}, \end{aligned}$$

and thus

$$f(x)g(x) = \sum_{n=0}^{r+s} a_n x^n,$$

where

$$a_n = \sum_{j=\max(0,n-s)}^{\min(r,n)} b_j c_{n-j}$$

for $n = 0, 1, 2, \ldots, r + s$. The operations of addition and multiplication of polynomials defined in this fashion satisfy the usual Commutative, Associative and Distributive Laws. Each element r of the coefficient ring R determines a corresponding polynomial of degree zero with coefficients are given by the infinite sequence $r, 0_R, 0_R, 0_R, 0_R, \ldots$, where 0_R denotes the zero element of the ring R. This polynomial is the *constant polynomial* in $R[x]$ with coefficient r. It is customary to use the same symbol to represent both the element r of the coefficient ring R and also the corresponding constant polynomial.

In particular, the zero element 0_R and the multiplicative identity element 1_R of the coefficient ring R determine corresponding constant polynomials, also denoted by 0_R and 1_R. Moreover $f(x) + 0_R = f(x)$ and $f(x)1_R = f(x)$ for all polynomials f with coefficients in the ring R. Also each polynomial $f(x)$ with coefficients in R determines a corresponding polynomial $-f(x)$ with the property that $f(x) + (-f(x)) = 0_R$: if

$$f(x) = a_0 + a_1 x + x_2 x^2 + \cdots + a_{m-1} x^{m-1} + a_m x^m$$

then

$$-f(x) = (-a_0) + (-a_1)x + (-a_2)x^2 + \cdots + (-a_{m-1})x^{m-1} + (-a_m)x^m.$$

The results described above ensure that the set $R[x]$ of polynomials with coefficients in the ring R, with the operations of addition and multiplication of polynomials defined as described above, is itself a unital commutative ring. Moreover there is a standard embedding of the coefficient ring R into the polynomial ring $R[x]$: the coefficient ring R is naturally isomorphic to the subring of $R[x]$ whose elements are constant polynomials, and we can therefore identity each element of the coefficient ring R with the constant polynomial that it determines.

Lemma 1.9 *Let K be a field, and let $f \in K[x]$ be a non-zero polynomial with coefficients in K. Then, given any polynomial $h \in K[x]$, there exist unique polynomials q and r in $K[x]$ such that $h = fq + r$ and either $r = 0$ or else* $\deg r < \deg f$.

Proof If $\deg h < \deg f$ then we may take $q = 0$ and $r = h$. In general we prove the existence of q and r by induction on the degree $\deg h$ of h. Thus suppose that $\deg h \geq \deg f$ and that any polynomial of degree less than $\deg h$ can be expressed in the required form. Now there is some element c of K for which the polynomials $h(x)$ and $cf(x)$ have the same leading coefficient. Let $h_1(x) = h(x) - cx^m f(x)$, where $m = \deg h - \deg f$. Then either $h_1 = 0$ or $\deg h_1 < \deg h$. The inductive hypothesis then ensures the existence of polynomials q_1 and r such that $h_1 = fq_1 + r$ and either $r = 0$ or else $\deg r < \deg f$. But then $h = fq + r$, where $q(x) = cx^m + q_1(x)$. We now verify the uniqueness of q and r. Suppose that $fq + r = f\overline{q} + \overline{r}$, where $\overline{q}, \overline{r} \in K[x]$ and either $\overline{r} = 0$ or $\deg \overline{r} < \deg f$. Then $(q - \overline{q})f = r - \overline{r}$. But $\deg((q - \overline{q})f) \geq \deg f$ whenever $q \neq \overline{q}$, and $\deg(r - \overline{r}) < \deg f$ whenever $r \neq \overline{r}$. Therefore the equality $(q - \overline{q})f = r - \overline{r}$ cannot hold unless $q = \overline{q}$ and $r = \overline{r}$. This proves the uniqueness of q and r. ∎

Any polynomial f with coefficients in a field K generates an ideal (f) of the polynomial ring $K[x]$ consisting of all polynomials in $K[x]$ that are divisible by f.

Lemma 1.10 *Let K be a field, and let I be an ideal of the polynomial ring $K[x]$. Then there exists $f \in K[x]$ such that $I = (f)$, where (f) denotes the ideal of $K[x]$ generated by f.*

Proof If $I = \{0\}$ then we can take $f = 0$. Otherwise choose $f \in I$ such that $f \neq 0$ and the degree of f does not exceed the degree of any non-zero polynomial in I. Then, for each $h \in I$, there exist polynomials q and r in $K[x]$ such that $h = fq + r$ and either $r = 0$ or else $\deg r < \deg f$. (Lemma 1.9). But $r \in I$, since $r = h - fq$ and h and f both belong to I. The choice of f then ensures that $r = 0$ and $h = qf$. Thus $I = (f)$. ∎