

§35 Substitution and Differentiation

In this paragraph, we study the divisibility of polynomials by those of the first degree. We prove the familiar remainder theorem. Roots of polynomials are introduced and multiple roots are examined.

Everything in this paragraph is based on the substitution homomorphism which we now define.

35.1 Definition: Let R be a ring and let $f = \sum_{i=0}^n a_i x^i$ be an arbitrary polynomial in $R[x]$. Let S be a ring containing R . For any $s \in S$, the element $\sum_{i=0}^n a_i s^i$ of S is called the *value of f at s* . The value of f at s is said to be obtained by *substituting s for x* or by *evaluating f at s* . The value $\sum_{i=0}^n a_i s^i$ of f at s will be denoted by $f(s)$.

In many cases, S is taken to be R , and then $f(s) \in S$. In fact, we may always assume $S = R$ by taking f as a polynomial in $S[x]$. However, if $R \subset S$ and $s \in S \setminus R$, then $f(s)$ need not belong to R .

35.2 Examples: (a) Let $g = 4x^2 + 6x + 8 \in E[x]$, where E is the ring of even integers; so $E \subseteq \mathbb{Z}$. Now $1 \in \mathbb{Z}$ and $g(1) = 4 \cdot 1^2 + 6 \cdot 1 + 8 = 18 \in \mathbb{Z}$.

(b) Let $h = 3x^3 + 4x^2 + x - 1 \in \mathbb{Z}[x]$. Here \mathbb{Q} is a ring that contains \mathbb{Z} and $\frac{2}{5} \in \mathbb{Q}$. We have $h(\frac{2}{5}) = 3(\frac{2}{5})^3 + 4(\frac{2}{5})^2 + (\frac{2}{5}) - 1 = \frac{29}{125} \in \mathbb{Q}$.

(c) Let $f = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}x^2 + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}x + \begin{pmatrix} -1 & 0 \\ 2 & 0 \end{pmatrix} \in (\text{Mat}_2(\mathbb{Z}))[x]$. Now $\text{Mat}_2(\mathbb{Z})$ is a ring containing $\text{Mat}_2(\mathbb{Z})$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \text{Mat}_2(\mathbb{Z})$. Then $f\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right)$

$$= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 + \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 4 & 0 \end{pmatrix} \in \text{Mat}_2(\mathbb{Z}).$$

(d) Let R be a ring with identity and $f = \sum_{i=0}^{\infty} a_i x^i \in R[x]$. Then $R \subseteq R[x]$ and

$x \in R[x]$. The value of f at $x \in R[x]$ is $f(x) = \sum_{i=0}^{\infty} a_i x^i = f$, so $f(x) = f \in R[x]$.

From now on, the notations f and $f(x)$ for a polynomial in $R[x]$ will be used interchangeably.

(e) Again let R be a ring with identity and $f = \sum_{i=0}^{\infty} a_i x^i \in R[x]$ be a

polynomial with coefficients in R . Let y be an indeterminate distinct from x . Then R is contained in $R[y]$ and $y \in R[y]$. The value of f at y is

$$f(y) = \sum_{i=0}^{\infty} a_i y^i \in R[y].$$

(f) Let $p = x^3 - x + 1 \in \mathbb{Q}[x]$. Now $\mathbb{Q} \subseteq \mathbb{Q}[x]$, $x + 1 \in \mathbb{Q}[x]$ and $p(x + 1) = (x + 1)^3 - (x + 1) + 1 = x^3 + 3x^2 + 2x + 1 \in \mathbb{Q}[x]$. Similarly $x^2 \in \mathbb{Q}[x]$ and $p(x^2) = (x^2)^3 - (x^2) + 1 = x^6 - x^2 + 1 \in \mathbb{Q}[x]$.

(g) Let R be a ring. For any $f \in R[x]$, the value of f at $g \in R[x]$ can be found as in the last example, and it is a polynomial $f(g(x))$ in $R[x]$.

(h) Let $f = \bar{3}x^2 - \bar{5}x + \bar{2} \in \mathbb{Z}_{12}[x]$. The value $f(1)$ of f at $1 \in \mathbb{Z}$ is not defined, for \mathbb{Z} does not contain \mathbb{Z}_{12} .

(i) Let $q = x^2 + x + 2$ and $r = x^3 + x + 3 \in \mathbb{Z}[x]$. We put $t = qr = x^5 + x^4 + 3x^3 + 4x^2 + 5x + 6 \in \mathbb{Z}[x]$. One checks easily that $q(2) = 8$, $r(2) = 13$, $t(2) = 104$. Notice $t(2) = 8 \cdot 13 = q(2) \cdot r(2)$. This is explained in the next lemma.

35.3 Lemma: *Let R be a ring, S a ring that contains R , and s an element of S . If S is commutative, then the mapping*

$$\begin{aligned} T_s: R[x] &\rightarrow S \\ f &\rightarrow f(s) \end{aligned}$$

is a ring homomorphism (called the *substitution* or *evaluation homomorphism*).

Proof: For any $f = \sum_{i=0}^m a_i x^i$, $g = \sum_{j=0}^n b_j x^j$ in $R[x]$, we have

$$\begin{aligned} (f+g)T_s &= \left(\sum_{i=0}^m a_i x^i + \sum_{j=0}^n b_j x^j \right) T_s \\ &= \left(\sum_{i=0}^m (a_i + b_i) x^i \right) T_s \quad (\text{assuming } n = m \text{ without loss of generality}) \\ &= \sum_{i=0}^m (a_i + b_i) s^i \\ &= \sum_{i=0}^m a_i s^i + \sum_{i=0}^m b_i s^i \\ &= f(s) + g(s) \\ &= fT_s + gT_s, \end{aligned}$$

and further

$$\begin{aligned} (fg)T_s &= \left[\sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) x^k \right] T_s = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) s^k, \\ (fT_s)(gT_s) &= \left(\sum_{i=0}^m a_i x^i \right) T_s \cdot \left(\sum_{j=0}^n b_j x^j \right) T_s = \left(\sum_{i=0}^m a_i s^i \right) \cdot \left(\sum_{j=0}^n b_j s^j \right) \\ &= \sum_{i,j} a_i s^i b_j s^j \\ &= \sum_{i,j} a_i b_j s^{i+j} \quad (\text{using commutativity of } S) \\ &= \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) s^k \\ &= (fg)T_s. \end{aligned}$$

Hence T_s preserves sums and products, and is therefore a ring homomorphism. □

In the proof of Lemma 35.3, the commutativity of S is used in a crucial way. If S is not commutative, then T_s is *not* a homomorphism. For example,

$$Ix^2 - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = [Ix + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}][Ix - \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}] \quad \text{in } (Mat_2(\mathbb{Z}))[x]$$

but substituting $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ for x does not preserve sums and products:

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}^2 - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \neq [\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}][\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}].$$

The substitution homomorphism is closely related to the division algorithm in an integral domain.

35.4 Theorem (Remainder theorem): *Let D be an integral domain, $f \in D[x]$ and $a \in D$. There is a unique polynomial q in $D[x]$ such that*

$$f(x) = q(x)(x - a) + f(a).$$

Proof: We divide f by $(x - a)$. This is possible by Theorem 34.4, because the leading coefficient of $x - a$ is a unit in D (in fact = 1). Thus there are unique polynomials q and r such that

$$f(x) = q(x)(x - a) + r(x) \quad r = 0 \text{ or } \deg r < \deg(x - a) = 1.$$

So r is an element of D (zero or not). To find r , we substitute a for x ; since substitution is a homomorphism by Lemma 35.3, we get

$$\begin{aligned} f(a) &= q(a)(a - a) + r(a) \\ f(a) &= r. \end{aligned}$$

This completes the proof. □

35.5 Definition: Let R be a ring, S a commutative ring that contains R and let f be a polynomial in $R[x]$. An element a of S is called a *root* or *zero of f* if $f(a) = 0$.

35.6 Theorem (Factor theorem): *Let D be an integral domain, and let f be an arbitrary polynomial in $D[x]$. Let E be an integral domain containing D and let $a \in E$. Then a is a root of f if and only if $(x - a)|f$ in $E[x]$.*

Proof: By the remainder theorem (with E in place of D), there is a polynomial q in $E[x]$ such that $f(x) = q(x)(x - a) + f(a)$. If a is a root of f , then $f(a) = 0$, so $f(x) = q(x)(x - a)$ and $(x - a)|f(x)$ in $E[x]$. Conversely, if $(x - a)|f(x)$ in $E[x]$, then $(x - a)|[f(x) - q(x)(x - a)]$ in $E[x]$, so $(x - a)|f(a)$ in $E[x]$. Thus $f(x) = u(x)(x - a)$ for some $u(x) \in E[x]$. Substituting a for x , we get $f(a) = u(a)(a - a) = 0$. So a is a root of f . \square

The factor theorem puts an upper bound to the number of roots of polynomials over integral domains, in particular of those over fields.

35.7 Theorem: *Let D be an integral domain, f a nonzero polynomial in $D[x]$ and let E be an integral domain containing D . Then there are at most $\deg f$ distinct roots of f in E .*

Proof: We make induction on the degree of f . Polynomials of degree 0 are just the nonzero elements of D , and they have no roots in E (zero roots). So the theorem is true when $\deg f = 0$. Assume now $\deg f = 1$, so that $f = cx + d$, where $c, d \in D$ and $c \neq 0$. If f had more than one roots in E , say if a_1, a_2 were roots of f in E and $a_1 \neq a_2$, we would get

$$\begin{aligned} ca_1 + d = f(a_1) = 0 = f(a_2) = ca_2 + d \\ ca_1 = ca_2 \\ c(a_1 - a_2) = 0 \quad c \neq 0 \\ a_1 - a_2 = 0, \end{aligned}$$

contrary to $a_1 \neq a_2$. Thus $cx + d$ has either no roots in E or one and only one root in E , and the theorem is proved when $\deg f = 1$.

Suppose now $n \geq 2$, $\deg f = n$ and that, for all integral domains D' , any polynomial of degree $n - 1$ in $D'[x]$ has at most $n - 1$ distinct roots in any integral domain E' that contains D' . If f has no roots in E , the theorem is true. If f has a root a_0 in E , we have

$$f(x) = q(x)(x - a_0) \quad \text{for some } q(x) \in E[x]$$

by the factor theorem. Here $q(x)$ is of degree $n - 1$ by Lemma 33.3(3). By our induction hypothesis, $q(x)$ has at most $n - 1$ distinct roots in E . Now let A be the set of all distinct roots of $q(x)$ in E (possibly $A = \emptyset$) so that $|A| \leq n - 1$.

If $b \in E$ is any root of f , then $f(b) = 0$, so $q(b)(b - a_0) = 0$, so $q(b) = 0$ or $b = a_0$, so $b \in A$ or $b = a_0$. Hence $B \subseteq A \cup \{a_0\}$, where B is the set of all distinct roots of $f(x)$ in E . Thus $|B| \leq |A| + 1 \leq (n - 1) + 1 = n$ and f has at most $n = \deg f$ distinct roots in E . This completes the proof. \square

Theorem 35.7 may be false if the underlying ring is not commutative or if it has zero divisors. For example, $x^2 + 1 \in H[x]$ of degree two over the noncommutative ring H of Ex. 9 in §29 has infinitely many roots in H . Also, the polynomial $x^2 - 1 = \bar{1}x^2 - \bar{1}$ over \mathbb{Z}_8 , which has zero divisors, possesses four distinct roots $\bar{1}, \bar{3}, \bar{5}, \bar{7}$ in \mathbb{Z}_8 .

We give two applications of Theorem 35.7. In these applications, the underlying integral domain is a field.

35.8 Theorem (Lagrange's interpolation formula): *Let K be a field and a_0, a_1, \dots, a_n be distinct elements of K . Let b_0, b_1, \dots, b_n be arbitrary elements of K (not necessarily distinct). Then there is a unique polynomial in $K[x]$ such that $f(a_0) = b_0, f(a_1) = b_1, \dots, f(a_n) = b_n$ and such that $\deg f \leq n$ (one less than the number of a 's or b 's) or $f = 0$. This polynomial is given explicitly by the formula*

$$f = \sum_{i=0}^n \frac{(x - a_0) \cdots (x - a_{i-1})(x - a_{i+1}) \cdots (x - a_n)}{(a_i - a_0) \cdots (a_i - a_{i-1})(a_i - a_{i+1}) \cdots (a_i - a_n)} b_i$$

Proof: The i -th summand $f_i :=$

$$\frac{(x - a_0) \cdots (x - a_{i-1})(x - a_{i+1}) \cdots (x - a_n)}{(a_i - a_0) \cdots (a_i - a_{i-1})(a_i - a_{i+1}) \cdots (a_i - a_n)} b_i$$

in the formula is $0 \in K[x]$ (when $b_i = 0$) or a polynomial in $K[x]$ of degree n (when $b_i \neq 0$). Here $f_i(a_i) = b_i$ and $f_i(a_j) = 0$ for $i \neq j$. So $f := f_1 + f_2 + \cdots + f_n$ is either the zero polynomial or a polynomial of degree at most n such that $f(a_i) = f_1(a_i) + f_2(a_i) + \cdots + f_n(a_i) = 0 + \cdots + f_i(a_i) + 0 + \cdots + 0 = b_i$ for all $i = 1, 2, \dots, n$. This proves the existence of a polynomial with the properties stated in the theorem, namely the one given explicitly above.

The uniqueness of f follows from Theorem 35.7. If g is a polynomial in $K[x]$ with $\deg g \leq n$, and if $g(a_1) = b_1, g(a_2) = b_2, \dots, g(a_n) = b_n$, then the

polynomial $h = f - g$ has at least $n + 1$ roots a_0, a_1, \dots, a_n in K , and, if $h \neq 0$, then h has degree at most equal to n (Lemma 33.3(2)). This is not compatible with Theorem 35.7, so $h = 0$ and $g = f$. Therefore f is the unique polynomial satisfying the conditions above. \square

The formula for f is easy to remember. We have $f = f_1 + f_2 + \dots + f_n$, where $f_i(a_i) = b_i$ and $f_i(a_j) = 0$ for $i \neq j$. The second condition leads to $f_i = (x - a_0) \dots (x - a_{i-1})(x - a_{i+1}) \dots (x - a_n)c_i$ for some $c_i \in K$, and c_i must be as in the formula if $f_i(a_i)$ is to be equal to b_i .

35.9 Theorem (Wilson's theorem): *If $p \in \mathbb{N}$ is a prime number, then $(p - 1)! + 1 \equiv 0 \pmod{p}$.*

Proof (Lagrange): Fermat's theorem (Theorem 12.6) states that $a^{p-1} \equiv 1 \pmod{p}$ for any integer a with $(a, p) = 1$. We can write this as

$$\overline{a^{p-1}} - \overline{1} = \overline{0} \quad \text{in } \mathbb{Z}_p \quad \text{if } \overline{a} \neq \overline{0}.$$

Thus the polynomial $f = x^{p-1} - \overline{1} = \overline{1}x^{p-1} - \overline{1} \in \mathbb{Z}_p[x]$ has $p - 1$ distinct roots in \mathbb{Z}_p , namely $\overline{1}, \overline{2}, \dots, \overline{p - 1}$. The polynomial

$$g = (x - \overline{1})(x - \overline{2}) \dots (x - \overline{p - 1})$$

has the same roots. Hence the polynomial

$$h = f - g = (\overline{1}x^{p-1} - \overline{1}) - (x - \overline{1})(x - \overline{2}) \dots (x - \overline{p - 1}) = (x^{p-1} - \overline{1}) - (x^{p-1} + \dots)$$

over \mathbb{Z}_p has at least $p - 1$ roots $\overline{1}, \overline{2}, \dots, \overline{p - 1}$ in \mathbb{Z}_p . If h were not the zero polynomial in $\mathbb{Z}_p[x]$, its degree would be less than $p - 1$. This contradicts Theorem 35.7. So h is the zero polynomial in $\mathbb{Z}_p[x]$: each coefficient of h is equal to $\overline{0} \in \mathbb{Z}_p$. In particular,

$$\begin{aligned} \overline{0} &= \text{coefficient of } x^0 \text{ in } h \\ &= (\text{coefficient of } x^0 \text{ in } f) - (\text{coefficient of } x^0 \text{ in } g) \\ &= (-\overline{1}) - ((-\overline{1})(-\overline{2}) \dots (-\overline{p - 1})) \\ &= -\overline{1} - (-1)^{p-1}(\overline{p - 1})! \\ &= -((\overline{p - 1})! + \overline{1}) \text{ in } \mathbb{Z}_p \end{aligned}$$

provided p is odd. Hence $(p - 1)! + 1 \equiv 0 \pmod{p}$ when p is an odd prime number. But this congruence holds also when $p = 2$. This completes the proof. \square

The next theorem will be familiar to the reader in the case of $D = \mathbb{Z}$, $F = \mathbb{Q}$ under the name of "rational root theorem".

35.10 Theorem: *Let D be a unique factorization domain and let F be the field of fractions of D . Let $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in D[x]$ be an arbitrary polynomial in $D[x]$. If $a = \frac{b}{c} \in F$ is a root of f , where $b, c \in D$ and $(b, c) \approx 1$, then*

$$c|a_n \quad \text{and} \quad b|a_0 \quad \text{in } D.$$

In particular, if the leading coefficient of f is a unit in D , then any root of f in F is actually in D .

Proof: By hypothesis, $a = \frac{b}{c}$ is a root of f so that

$$a_n \frac{b^n}{c^n} + a_{n-1} \frac{b^{n-1}}{c^{n-1}} + \cdots + a_1 \frac{b}{c} + a_0 = 0.$$

Multiplying both sides by c^n , we obtain

$$\begin{aligned} a_n b^n + (a_{n-1} b^{n-1} c + \cdots + a_1 b c^{n-1} + a_0 c^n) &= 0, \\ [a_n b^n + a_{n-1} b^{n-1} c + \cdots + a_1 b c^{n-1}] + a_0 c^n &= 0. \end{aligned}$$

c divides the expression in (), so $c|a_n b^n$. As $(b, c) \approx 1$, we have $(b^n, c) \approx 1$. From $(b^n, c) \approx 1$ and $c|a_n b^n$, we conclude $c|a_n$. Likewise, b divides the expression in [], so $b|a_0 c^n$. As $(b, c) \approx 1$, we have $(b, c^n) \approx 1$. From $(b, c^n) \approx 1$ and $b|a_0 c^n$, we conclude $b|a_0$. In particular, if a_n is a unit in D , then c is also a unit in D since $c|a_n$, so there is a $c^{-1} \in D$ such that $cc^{-1} = 1$ and the

$$\text{root } a = \frac{b}{c} = \frac{bc^{-1}}{cc^{-1}} = \frac{bc^{-1}}{1} = bc^{-1} \in D. \quad \square$$

35.11 Example: As an illustration of Theorem 35.10, we prove that the real number $\sqrt{2}$ is irrational. Let $f(x) = x^2 - 2 \in \mathbb{Z}[x]$. Since \mathbb{Z} is a unique factorization domain and the leading coefficient of f is a unit in \mathbb{Z} (f is in

fact a monic polynomial), any root of f in \mathbb{Q} must be actually in \mathbb{Z} by Theorem 35.10. But

$$f(0) = -2 \neq 0; \quad f(\mp 1) = -1 \neq 0;$$

$$f(\mp m) = m^2 - 2 \geq 2, \text{ so } f(\mp m) \neq 0 \text{ for } m \geq 2;$$

so f has no integer roots, and consequently no rational roots, as claimed.

Next we discuss the multiplicity of roots. Let D be an integral domain and f a nonzero polynomial in $D[x]$. If $a \in D$ is a root of f , then we have $f(x) = (x - a)q_1(x)$ for some $q_1(x) \in D[x]$ by the factor theorem (Theorem 35.6). Either a is not a root of $q_1(x)$, or we have $q_1(x) = (x - a)q_2(x)$ and therefore $f(x) = (x - a)^2q_2(x)$ for some $q_2(x) \in D[x]$. In the latter case, either a is not a root of $q_2(x)$, or we have $q_2(x) = (x - a)q_3(x)$ and therefore $f(x) = (x - a)^3q_3(x)$ for some $q_3(x) \in D[x]$. We repeat this argument. Since the degrees of $q_1(x), q_2(x), q_3(x), \dots$ get smaller and smaller, we will reach a polynomial $q_m(x)$ with

$$f(x) = (x - a)^m q_m(x), \quad q_m(a) \neq 0.$$

35.12 Definition: Let D be an integral domain and f a nonzero polynomial in $D[x]$. Suppose $a \in D$ and $f(a) = 0$. The uniquely determined integer $m \geq 1$ such that

$$f(x) = (x - a)^m q_m(x), \quad q_m(x) \in D[x], \quad q_m(a) \neq 0,$$

that is, the uniquely determined integer $m \geq 1$ such that

$$(x - a)^m | f(x), \quad (x - a)^{m+1} \nmid f(x) \quad \text{in } D[x]$$

is called the *multiplicity* of the root a of f . The root a of f is called a *simple* root when $m = 1$ and a *multiple* root when $m > 1$.

This definition makes sense also when a is a root of f in E , where E is an integral domain containing D : we need only regard f as a polynomial over E and use the definition with E in place of D . When E_1 and E_2 are two integral domains containing D and a root a of f is both in E_1 and E_2 , we have, say,

$$\begin{aligned} f(x) &= (x - a)^{m_1} q_1(x), & q_1(x) &\in E_1[x], & q_1(a) &\neq 0, \\ f(x) &= (x - a)^{m_2} q_2(x), & q_2(x) &\in E_2[x], & q_2(a) &\neq 0, \\ f(x) &= (x - a)^{m_0} q_0(x), & q_0(x) &\in (E_1 \cap E_2)[x], & q_0(a) &\neq 0, \end{aligned}$$

as the equations defining the multiplicity of a as a root in $E_1, E_2, E_1 \cap E_2$.

Then

$$(x - a)^{m_1} q_1(x) = (x - a)^{m_0} q_0(x) \quad \text{in } E_1[x]$$

and the assumption $m_1 > m_0$ or $m_1 < m_0$ leads to the contradiction

$$\begin{aligned} (x - a)^{m_1 - m_0} q_1(x) &= q_0(x) \quad \text{or} \quad q_1(x) = (x - a)^{m_0 - m_1} q_0(x), \\ 0 &= q_0(a) \quad \text{or} \quad q_1(a) = 0. \end{aligned}$$

Hence $m_1 = m_0$. Likewise $m_2 = m_0$ and therefore $m_1 = m_2$: the multiplicity of a root of $f \in D[x]$ is independent of the integral domain to which the root belongs.

In order to find out whether a polynomial has multiple roots, we take derivatives.

In analysis, the derivative of a real-valued function u of a real variable x is defined by

$$u'(x) = \lim_{h \rightarrow 0} \frac{u(x + h) - u(x)}{h}.$$

This definition cannot be extended to polynomials over a ring. For one thing, polynomials are not functions. Second, what should

$\frac{u(x + h) - u(x)}{h}$ mean in a ring? Third, we did not define limits in a ring. In fact, in many rings, a reasonable limit process cannot be introduced at all. But we know from analysis that the derivative of the function $x \rightarrow \sum_{k=0}^n a_k x^k$ is the function $x \rightarrow \sum_{k=1}^n k a_k x^{k-1}$. This suggests the

following definition.

35.13 Definition: Let R be an arbitrary ring and let $f = \sum_{k=0}^n a_k x^k$ be an arbitrary polynomial in $R[x]$. The *derivative of f* is defined as the polynomial

$$f' = f'(x) = \sum_{k=1}^n k a_k x^{k-1} = \sum_{k=0}^{n-1} (k+1) a_k x^{k-1} \in R[x].$$

$k a_k$ means of course $a_k + a_k + \dots + a_k$ in R (k times). This definition has nothing to do with limits. Taking the derivative of a polynomial is called differentiation.

35.14 Examples: (a) Let $f(x) = x^4 - 3x^2 + x + 10 \in \mathbb{Z}[x]$. Then $f'(x) = 4x^3 - 6x + 1 \in \mathbb{Z}[x]$.

(b) Let $g(x) = \frac{1}{3}x^5 + \frac{1}{7}x^4 + \frac{2}{5}x^3 + \frac{4}{3}x - 3 \in \mathbb{Q}[x]$. Then

$$g'(x) = \frac{5}{3}x^4 + \frac{4}{7}x^3 + \frac{6}{5}x^2 + \frac{4}{3} \in \mathbb{Q}[x].$$

(c) Let $h(x) = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} x^3 + \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} x^2 + \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} x + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in (\text{Mat}_2(\mathbb{Z}))[x]$. Then

$$\begin{aligned} h'(x) &= 3 \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} x^2 + 2 \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} x + 1 \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 3 & 6 \\ 9 & 12 \end{pmatrix} x^2 + \begin{pmatrix} 0 & 2 \\ -2 & 2 \end{pmatrix} x + \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \in (\text{Mat}_2(\mathbb{Z}))[x]. \end{aligned}$$

(d) Let $k(x) = \bar{2}x^4 + \bar{4}x^2 + \bar{3}x + \bar{5} \in \mathbb{Z}_8[x]$. Then

$$k'(x) = 4 \cdot \bar{2}x^3 + 2 \cdot \bar{4} + 1 \cdot \bar{3} = \bar{3} \in \mathbb{Z}_8[x].$$

(e) Let $l(x) = x^{125} + x^{25} + \bar{2}x^5 + \bar{3} \in \mathbb{Z}_5[x]$. Then

$$l'(x) = 125 \cdot \bar{1}x^{124} + 25 \cdot \bar{1}x^{24} + 5 \cdot \bar{2}x^4 = 0 \in \mathbb{Z}_5[x].$$

The familiar rules of differentiation hold in any polynomial ring.

35.15 Lemma: Let R be a ring, $c \in R$, and let $f, g \in R[x]$. Then

$$(f+g)' = f' + g', \quad (cf)' = cf', \quad (fg)' = f'g + fg'.$$

Proof: Let $f = \sum_{k=0}^m a_k x^k$ and $g = \sum_{j=0}^n b_j x^j$. We have

$$\begin{aligned}
 (f+g)' &= \left(\sum_{k=0}^m a_k x^k + \sum_{j=0}^n b_j x^j \right)' \\
 &= \left(\sum_{k=0}^m a_k x^k + \sum_{k=0}^m b_k x^k \right)' \text{ (assuming } n = m \text{ without loss of} \\
 &\text{generality)} \\
 &= \left(\sum_{k=0}^m (a_k + b_k) x^k \right)' \\
 &= \sum_{k=1}^m k(a_k + b_k) x^{k-1} \\
 &= \sum_{k=1}^m (ka_k + kb_k) x^{k-1} \\
 &= \sum_{k=1}^m ka_k x^{k-1} + \sum_{k=1}^m kb_k x^{k-1} \\
 &= f' + g',
 \end{aligned}$$

$$(cf)' = \left(c \sum_{k=0}^m a_k x^k \right)' = \left(\sum_{k=0}^m ca_k x^k \right)' = \sum_{k=1}^m kca_k x^{k-1} = c \sum_{k=1}^m ka_k x^{k-1} = cf'$$

Next we find $(fg)'$ and $f'g + fg'$. We have

$$\begin{aligned}
 (fg)' &= \left[\left(\sum_{k=0}^m a_k x^k \right) \left(\sum_{j=0}^n b_j x^j \right) \right]' \\
 &= \left[\sum_{s=0}^{m+n} \left(\sum_{k+j=s} a_k b_j \right) x^s \right]' \\
 &= \sum_{s=1}^{m+n} s \left(\sum_{k+j=s} a_k b_j \right) x^{s-1},
 \end{aligned}$$

(1)

$$\begin{aligned}
 f'g + fg' &= \left(\sum_{k=0}^m a_k x^k \right)' \left(\sum_{j=0}^n b_j x^j \right) + \left(\sum_{k=0}^m a_k x^k \right) \left(\sum_{j=0}^n b_j x^j \right)' \\
 &= \left(\sum_{k=1}^m ka_k x^{k-1} \right) \left(\sum_{j=0}^n b_j x^j \right) + \left(\sum_{k=0}^m a_k x^k \right) \left(\sum_{j=1}^n jb_j x^{j-1} \right)
 \end{aligned}$$

$$\begin{aligned}
&= \sum_{s=1}^{m+n} \left(\sum_{k+j=s} ka_k b_j \right) x^{s-1} + \sum_{s=1}^{m+n} \left(\sum_{k+j=s} ja_k b_j \right) x^{s-1} \\
&= \sum_{s=1}^{m+n} \left(\sum_{k+j=s} ka_k b_j + ja_k b_j \right) x^{s-1} \\
&= \sum_{s=1}^{m+n} s \left(\sum_{k+j=s} a_k b_j \right) x^{s-1}.
\end{aligned}$$

(2)

From (1) and (2), we conclude $(fg)' = f'g + fg'$. This completes the proof.

□

35.16 Lemma: Let R be a ring and let $f_1, f_2, \dots, f_n, g \in R[x]$.

(1) $(f_1 + f_2 + \dots + f_n)' = f_1' + f_2' + \dots + f_n'$.

(2) $(f_1 f_2 \dots f_n)' = f_1' f_2 \dots f_n + f_1 f_2' \dots f_n + \dots + f_1 f_2 \dots f_n'$.

(3) $(g^n)' = n g^{n-1} g'$.

(4) $[f(g(x))]' = f'(g(x))g'(x)$.

Proof: (1) and (2) follow from Lemma 35.16 by induction on n . (3) is a special case of (2), with $f_1 = f_2 = \dots = f_n = g$. We now prove (4). Let

$f = \sum_{k=0}^m a_k x^k$. Then $f(g(x)) = \sum_{k=0}^m a_k g^k \in R[x]$ and, by (1) and (3), the

derivative of $f(g(x))$ is

$$\begin{aligned}
\left(\sum_{k=0}^m a_k g^k \right)' &= \sum_{k=0}^m a_k (g^k)' = \sum_{k=1}^m a_k (g^k)' = \sum_{k=1}^m ka_k g^{k-1} g' \\
&= \left(\sum_{k=1}^m ka_k g^{k-1} \right) g' = f'(g)g'.
\end{aligned}$$

□

We are now in a position to determine which roots are multiple roots.

35.17 Theorem: Let D be an integral domain, and E an integral domain that contains D . Let $c \in E$ and let f be a nonzero polynomial in $D[x]$. Then c is a multiple root of f if and only if c is a root of both f and f' .

Proof: Suppose c is a multiple root of f . Then it is a root of f . We wish to show that c is a root of f' as well. We have $f(x) = (x - c)^2g(x)$ for some $g(x) \in E[x]$. Differentiating and substituting c for x , we obtain

$$\begin{aligned} f'(x) &= 2(x - c)g(x) + (x - c)^2g'(x) \\ f'(c) &= 2(c - c)g(c) + (c - c)^2g'(c) = 0 \end{aligned}$$

and c is indeed a root of f' .

Conversely, suppose c is a root of f and f' . We write $f(x) = (x - c)h(x)$, where $h(x) \in E[x]$. We want to show that c is a root of h . Since

$$\begin{aligned} f'(x) &= h(x) + (x - c)h'(x) \\ f'(c) &= h(c) + (c - c)h'(c) \\ 0 &= h(c) + 0, \end{aligned}$$

$h(c) = 0$ and c is a multiple root of f . □

35.18 Theorem: Let K be a field and E an integral domain that contains K . Let $f(x), g(x)$ be arbitrary nonzero polynomials in $K[x]$.

(1) If f and g are relatively prime, then f and g have no common root in E .

(2) If f and f' are relatively prime, then f has no multiple roots in E .

(3) If f is irreducible in $K[x]$, then either f and g are relatively prime or $f|g$ in $K[x]$.

(4) If f is irreducible in $K[x]$ and $\deg f > \deg g$, then f and g have no common root in E .

(5) If f is irreducible in $K[x]$ and $f' \neq 0$, then there is no root of f in E which is a multiple root.

(6) If f is irreducible in $K[x]$ and if f has a root in E which is not a multiple root of f , then $f' \neq 0$.

Proof: (1) Suppose f and g are relatively prime in $K[x]$. By Theorem 34.6, there are polynomials h, l in $K[x]$ such that

$$1 = h(x)f(x) + l(x)g(x),$$

where 1 is the identity element of K . If f and g had a root $c \in E$ in common, we would have

$$1 = h(c)f(c) + l(c)g(c) = h(c)0 + l(c)0 = 0 + 0 = 0,$$

a contradiction. So f and g have no common root in E .

(2) Assume f and f' are relatively prime. If f has no root in E , then certainly f has no multiple root in E . Now we suppose f has a root c in E

and prove that c is not a multiple root of f . Indeed, since f and f' are relatively prime, f and f' have no common root by part (1), so $f'(c) \neq 0$ and c is not a multiple root of f by Theorem 35.17.

(3) Suppose f is irreducible in $K[x]$ and let $d \in K[x]$ be a greatest common divisor of f and g . Since $d|f$ and f is irreducible, d is either a unit in $K[x]$ or an associate of f . In the first case, f and g are relatively prime, in the second case, $f \approx d$ and $d|g$ yields $f|g$.

(4) Suppose f is irreducible in $K[x]$ and $\deg g < \deg f$, then f cannot divide g , so f and g are relatively prime by part (3). By part (1), f and g have no common root in E .

(5) Suppose f is irreducible in $K[x]$ and $f' \neq 0$. Then $\deg f' < \deg f$. Since f is irreducible, f and f' have no common root in E by part (4). Now if f has no root in E , then f has certainly no multiple root in E . If f has a root c in E , then c is not a root of f' , so c is not a multiple root of f by Theorem 35.17. In any case, f has no multiple root in E .

(6) Suppose f is irreducible in $K[x]$ and suppose $c \in E$ is a simple root of f in E . If we had $f' = 0$, we would have $f(c) = 0$ and $f'(c) = 0$ and c would be a multiple root of f by Theorem 35.17, a contradiction. Thus, if there are roots in E and if they are all simple, then $f' \neq 0$. \square

We finish this paragraph with a brief discussion of successive substitutions.

35.19 Definition: Let R be a ring and let

$$f = \sum_{i=0}^{N_1} \sum_{j=0}^{N_2} \dots \sum_{k=0}^{N_{n-1}} \sum_{l=0}^{N_n} a_{ij\dots kl} x_1^i x_2^j \dots x_{n-1}^k x_n^l$$

be a polynomial in $R[x_1, x_2, \dots, x_{n-1}, x_n]$. Let S be a ring that contains R and let $c_1, c_2, \dots, c_{n-1}, c_n$ be elements of S . The element

$$\sum_{i=0}^{N_1} \sum_{j=0}^{N_2} \dots \sum_{k=0}^{N_{n-1}} \sum_{l=0}^{N_n} a_{ij\dots kl} c_1^i c_2^j \dots c_{n-1}^k c_n^l$$

of S is called the *value of f at $(c_1, c_2, \dots, c_{n-1}, c_n)$* . It will be denoted by $f(c_1, c_2, \dots, c_{n-1}, c_n)$.

With the foregoing notation, $f = \sum_{i=0}^{N_1} \left(\sum_{j=0}^{N_2} \cdots \sum_{k=0}^{N_{n-1}} \sum_{l=0}^{N_n} a_{ij\dots kl} x_1^i x_2^j \cdots x_{n-1}^k \right) x_n^l$ is a polynomial in $R[x_1, x_2, \dots, x_{n-1}][x_n]$. Substituting c_n for x_n in the sense of Definition 35.1 (with $S[x_1, x_2, \dots, x_{n-1}]$, $R[x_1, x_2, \dots, x_{n-1}]$, x_n , c_n in place of S , R , x , c , respectively), we get an element of $S[x_1, x_2, \dots, x_{n-1}]$, namely

$$\sum_{i=0}^{N_1} \sum_{j=0}^{N_2} \cdots \sum_{k=0}^{N_{n-1}} \left(\sum_{l=0}^{N_n} c_n^l a_{ij\dots kl} \right) x_1^i x_2^j \cdots x_{n-1}^k \in S[x_1, x_2, \dots, x_{n-2}][x_{n-1}].$$

Substituting c_{n-1} for x_{n-1} in this polynomial over $S[x_1, x_2, \dots, x_{n-2}]$, we get a polynomial in $S[x_1, x_2, \dots, x_{n-2}]$, namely

$$\sum_{i=0}^{N_1} \sum_{j=0}^{N_2} \cdots \sum_{j'=0}^{N_{n-2}} \left(\sum_{k=0}^{N_{n-1}} \sum_{l=0}^{N_n} c_{n-1}^k c_n^l a_{ij\dots j'kl} \right) x_1^i x_2^j \cdots x_{n-2}^{j'}.$$

We continue in this way. If S is commutative, we obtain $f(c_1, c_2, \dots, c_{n-1}, c_n)$ after n substitutions. Thus

$$f(c_1, c_2, \dots, c_{n-1}, c_n) = f T_{c_n} T_{c_{n-1}} \cdots T_{c_2} T_{c_1},$$

where $T_{c_n} : R[x_1, x_2, \dots, x_{n-1}, x_n] \longrightarrow S[x_1, x_2, \dots, x_{n-1}]$
 $T_{c_h} : S[x_1, x_2, \dots, x_{h-1}, x_h] \longrightarrow S[x_1, x_2, \dots, x_{h-1}] \quad (h = 2, \dots, n-1)$
and $T_{c_1} : S[x_1] \longrightarrow S$

are the substitution homomorphisms in the sense of Definition 35.1. Since the composition of homomorphisms is a homomorphism (Theorem 30.12), we obtain the following lemma.

35.20 Lemma: *Let R be a ring, S a ring that contains R , and $c_1, c_2, \dots, c_{n-1}, c_n$ elements of S . If S is commutative, then the mapping*

$$T_{(c_1, c_2, \dots, c_{n-1}, c_n)} : R[x_1, x_2, \dots, x_{n-1}, x_n] \longrightarrow S$$

$$f \longrightarrow f(c_1, c_2, \dots, c_{n-1}, c_n)$$

is a ring homomorphism (called the evaluation or substitution homomorphism). \square

Exercises

1. Let $f = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$. Prove that f is reducible over \mathbb{Q} if and only if f has an integer root.

2. Find a polynomial $f \in \mathbb{Q}[x]$ with $\deg f \leq 4$ satisfying

$$f(-2) = 9, \quad f(-1) = -2, \quad f(0) = 1, \quad f(1) = 4, \quad f(2) = 25.$$

3. Let p be a prime number of the form $4k + 1$. Using Wilson's theorem, show that $\frac{p-1}{2}!$ is a root of $x^2 + \bar{1} \in \mathbb{Z}_p[x]$.

4. Let R be a ring and $f = \sum_{i,j,k} a_{ijk} x^i y^j z^k \in R[x,y,z]$. The derivative of f ,

when f is regarded as a polynomial in $R[y,z][x]$, is called the *derivative of f with respect to x* and is written $\frac{\partial f}{\partial x}$. Thus $\frac{\partial f}{\partial x} = \sum_{\substack{i,j,k \\ i \geq 1}} i a_{ijk} x^{i-1} y^j z^k$. The

derivatives with respect to y and z are defined similarly. f is said to be *homogeneous of degree m* if $i + j + k = m$ for all i, j, k with $a_{ijk} \neq 0$. Prove the following assertions.

(a) Let t be an indeterminate over $R[x,y,z]$. If $f(x,y,z) \in R[x,y,z]$ is a homogeneous polynomial of degree m , then

$$f(tx,ty,tz) = t^m f(x,y,z) \in R[x,y,z,t]. \quad (*)$$

(b) Let t be an indeterminate over $R[x,y,z]$ and $f(x,y,z) \in R[x,y,z]$. If $(*)$ holds in $R[x,y,z,t]$, then $f(x,y,z)$ is a homogeneous polynomial of degree m .

(c) If $f(x,y,z) \in R[x,y,z]$ is a homogeneous polynomial of degree m , then

$$f(rx,ry,rz) = r^m f(x,y,z)$$

for all $r \in R$.

(d) If $f(x,y,z) \in \mathbb{Q}[x,y,z]$ and $f(rx,ry,rz) = r^m f(x,y,z)$ for all $r \in \mathbb{Q}$, then $f(x,y,z)$ is a homogeneous polynomial of degree m .

(e) Find a polynomial $f(x,y,z) \in \mathbb{Z}_5[x,y,z]$ such that

$$f(rx,ry,rz) = r^m f(x,y,z) \text{ for all } r \in \mathbb{Z}_5$$

and which is not homogeneous of degree m .

(f) If $f(x,y,z) \in R[x,y,z]$ is homogeneous of degree m , then

$$x \frac{\partial f}{\partial x} + y \frac{\partial f}{\partial y} + z \frac{\partial f}{\partial z} = mf.$$

5. Let R be a ring and $f \in R[x]$. The derivative of f is called the *second derivative of f* , and is written as f' or as $f^{(2)}$. More generally, the $(n+1)$ -st derivative of f is defined recursively as the derivative of the n -th derivative $f^{(n)}$ of f , and is written as $f^{(n+1)}$. Thus $f^{(n+1)} = (f^{(n)})'$. We write $f^{(1)}$ for f' and $f^{(0)} = f$. Prove that, for any $f, g \in R[x]$, any $c \in R$, any $n \in \mathbb{N}$

$$(f+g)^{(n)} = f^{(n)} + g^{(n)}, \quad (cf)^{(n)} = cf^{(n)},$$

$$(fg)^{(n)} = \sum_{k=0}^n \binom{n}{k} f^{(n-k)} g^{(k)}.$$

6. Let K be a field, f a nonzero polynomial of degree n in $K[x]$ and assume that $(n!)1_K \neq 0$, where 1_K is the identity of K . Show that

$$f(x+y) = \sum_{k=0}^n \frac{f^{(k)}(x)}{k!} y^k$$

in $K[x, y]$, where, of course, $\frac{f^{(k)}(x)}{k!}$ means $[(k!)1_K]^{-1}f^{(k)}(x)$.

7. Let p be a prime number and $f \in \mathbb{Z}_p[x]$. Show that $f' = 0$ if and only if $f(x) = g(x^p)$ for some $g \in \mathbb{Z}_p[x]$.

8. Let K be a field. We put $M = \text{Mat}_2(K)$ for brevity. Let us recall that the determinant of $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M$ is $ad - bc$ and that $A \in M$ is a unit in M if and only if $\det A$ is a unit in K .

Let $A(x), B(x) \in M[x]$ be nonzero polynomials and assume that the leading coefficient of $B(x)$ has a nonzero determinant. Show that there are uniquely determined polynomials $Q(x), R(x), Q^\dagger(x), R^\dagger(x)$ in $M[x]$ such that

$$A(x) = Q(x)B(x) + R(x), \quad R(x) = 0 \text{ or } \deg R(x) < \deg B(x).$$

and

$$A(x) = B(x)Q^\dagger(x) + R^\dagger(x), \quad R^\dagger(x) = 0 \text{ or } \deg R^\dagger(x) < \deg B(x).$$

$Q(x)$ and $R(x)$ are called the *right quotient* and *right remainder*, $Q^\dagger(x)$ and $R^\dagger(x)$ are called the *left quotient* and *left remainder* when $A(x)$ is divided by $B(x)$.

If $F(x) = F_n x^n + F_{n-1} x^{n-1} + \cdots + F_1 x + F_0 \in M[x]$ and $A \in M$, then

$$F(A) := F_n A^n + F_{n-1} A^{n-1} + \cdots + F_1 A + F_0 \in M$$

is called the *right value of $F(x)$ at A* and

$$F^\dagger(A) := A^n F_n + A^{n-1} F_{n-1} + \cdots + A F_1 + F_0 \in M$$

is called the *left value of $F(x)$ at A* . Prove that the right (resp. left) remainder of $F(x) \in M[x]$, when $F(x)$ is divided by $Ix - A$, is equal to $F(A)$ (resp. $F^\dagger(A)$).

9. Let R be a ring and $D_i : R[x] \rightarrow R[x]$ be functions ($i = 1, 2$) such that

$$D_i(f + g) = D_i f + D_i g \quad D_i(cf) = c D_i f, \quad D_i(fg) = (D_i f)g + fD_i(g)$$

for all $f, g \in R[x]$. Define $D : R[x] \rightarrow R[x]$ by

$$Df = D_1(D_2 f) - D_2(D_1 f).$$

Prove that

$$D(f + g) = Df + Dg \quad D(cf) = c Df, \quad D(fg) = (Df)g + fD(g)$$

for all $f, g \in R[x]$.