

SOLVED PROBLEMS: SECTION 1.4

9. Let D be an integral domain. Prove that if the polynomial ring $D[x]$ is a principal ideal domain, then D is a field.

Solution: For any nonzero element $a \in D$, consider the ideal $\langle x, a \rangle$ of $D[x]$. By assumption, this ideal is a principal ideal, generated by an element $f(x) \in D[x]$. But then $f(x)$ is a divisor of a , so $f(x) = d$ for some $d \in D$. On the other hand, d is a divisor of x , so $x = d(bx + c)$ for some $b, c \in D$. It follows that $db = 1$ and $dc = 0$, so d is invertible. Therefore $\langle x, a \rangle = D[x]$, so $1 = xg(x) + ah(x)$ for some $g(x), h(x) \in D[x]$. It follows that $ah(0) = 1$, so a is invertible, and D must be a field.

10. Let $f(x) = a_mx^m + \dots + a_1x + a_0$, $g(x) = b_nx^n + \dots + b_1x + b_0$, and $h(x) = c_kx^k + \dots + c_1x + c_0$ be polynomials in $\mathbf{Z}[x]$, with $f(x) = g(x)h(x)$. Let p be a prime number. Show that if b_s and c_t are the coefficients of $g(x)$ and $h(x)$ of least index not divisible by p , then a_{s+t} is the coefficient of $f(x)$ of least index not divisible by p .

Solution: Each of the coefficients b_0, b_1, \dots, b_{s-1} and c_{t-1}, \dots, c_0 is divisible by p , so in the coefficient

$$a_{s+t} = b_0c_{s+t} + b_1c_{s+t-1} + \dots + b_{s-1}c_{t+1} + b_sc_t + b_{s+1}c_{t-1} + \dots + b_{s+t}c_0$$

of $f(x)$, each term except b_sc_t is divisible by p . This implies that a_{s+t} is not divisible by p , and in any coefficient of $f(x)$ of lower degree, each term in the sum $a_k = \sum_{i=0}^k b_ic_{k-i}$ is divisible by p .

11. Prove Eisenstein's irreducibility criterion, which states that if $f(x) = a_nx^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbf{Z}[x]$ and there exists a prime number p such that $a_{n-1} \equiv a_{n-2} \equiv \dots \equiv a_0 \equiv 0 \pmod{p}$ but $a_n \not\equiv 0 \pmod{p}$ and $a_0 \not\equiv 0 \pmod{p^2}$, then $f(x)$ is irreducible over \mathbf{Q} .

Solution: Suppose that $f(x)$ can be factored as $f(x) = g(x)h(x)$, where $g(x) = b_mx^m + \dots + b_0$ and $h(x) = c_kx^k + \dots + c_0$. By Gauss's lemma (Lemma 1.4.8) we can assume that both factors have integer coefficients. Furthermore, we can assume that either b_0 or c_0 is not divisible by p , since $b_0c_0 = a_0$ is not divisible by p^2 . Suppose that $p \nmid b_0$. If c_t is the coefficient of $h(x)$ of least degree that is not divisible by p , then it follows from Exercise 10 that $a_t = a_{0+t}$ is the coefficient of $f(x)$ of least degree that is not divisible by p . Therefore $t = n$, showing that $h(x)$ and $f(x)$ have the same degree, and so $f(x)$ is irreducible.

or, equivalently, iff $p \equiv 1 \pmod{4}$.