

**Throughout,  $A$  is a commutative ring with  $0 \neq 1$ .**

1. Let  $k$  be a field, and  $k[x]$  a polynomial ring. Prove that  $k[x]$  contains infinitely many distinct monic irreducible polynomials.

**Solution:** If not, let  $f_1(x), \dots, f_n(x)$  be all the distinct monic irreducible polynomials in  $k[x]$ . But then

$$f(x) = f_1(x) \cdots f_n(x) + 1$$

is not divisible by any of  $f_1(x), \dots, f_n(x)$  so it must be irreducible, a contradiction.

2. Let  $S \subset \mathbb{Z}$  be the multiplicative set consisting of all positive odd integers. What are all ideals of  $S^{-1}\mathbb{Z}$ ?

**Solution:** Every element of  $S^{-1}\mathbb{Z}$  can be written uniquely as  $\pm 2^k m/n$ , where  $k \geq 0$  and  $m, n$  are relatively prime odd integers. Given a nonzero ideal  $\mathfrak{a} \subseteq S^{-1}\mathbb{Z}$ , let  $x = 2^k m/n$ , written as above, be the element of  $\mathfrak{a}$  with  $k$  least possible. It is easily seen that  $\mathfrak{a} = (x) = (2^k/1)$ . Consequently the ideals of  $S^{-1}\mathbb{Z}$  are the zero ideal and  $(2^k/1)$  for  $k \geq 0$ .

3. If  $A$  is a domain which is not a field, prove that  $A[x]$  is not a principal ideal domain.

**Solution:** There exists  $a \in A$  which is nonzero and is not a unit. We claim that the ideal  $\mathfrak{a} = (a, x) \subset A[x]$  is not principal. Indeed, if  $\mathfrak{a} = (f(x))$  for some  $f(x) \in A[x]$ , then  $a = g(x)f(x)$  for some  $g(x) \in A[x]$ , so  $f(x)$  has degree zero, i.e.,  $f(x) \in A$ . But then  $x \in (f(x))$  forces  $f(x)$  to be a unit, which is not possible since  $(a, x) \neq A[x]$ .

4. If every submodule of every free  $A$ -module is free, prove that  $A$  is a principal ideal domain.

**Solution:** First note that for nonzero  $a \in A$ , the module  $Aa \subseteq A$  is a submodule of a free module, and hence is free. Therefore  $ba \neq 0$  for all  $b \neq 0$ , and so  $A$  is a domain.

Let  $\mathfrak{a}$  be a nonzero ideal of  $A$ . Since it is a submodule of  $A$ , which is a free  $A$ -module,  $\mathfrak{a}$  must be free. If  $f, g \in \mathfrak{a}$  are part of a basis for  $\mathfrak{a}$ , then the relation  $-g(f) + f(g) = 0$  shows that  $f, g$  are not linearly independent, a contradiction. Hence a basis for  $\mathfrak{a}$  must consist of exactly one element  $f$ , but then  $\mathfrak{a} = Af$  is a principal ideal.

5. In which of the following rings is every ideal principal? Justify your answer.

$$(i) \mathbb{Z} \oplus \mathbb{Z}, \quad (ii) \frac{\mathbb{Z}}{(4)}, \quad (iii) \frac{\mathbb{Z}}{(6)}[x], \quad (iv) \frac{\mathbb{Z}}{(4)}[x].$$

**Solution:** Note that every ideal of the ring  $A \oplus B$  is of the form  $\mathfrak{a} \oplus \mathfrak{b}$  for ideals  $\mathfrak{a} \subset A$  and  $\mathfrak{b} \subset B$ . If  $\mathfrak{a} = (a)$  and  $\mathfrak{b} = (b)$ , then it is easily seen that  $\mathfrak{a} \oplus \mathfrak{b}$  is generated by the element  $(a, b) \in A \oplus B$ , hence is a principal ideal.

(i) Since  $\mathbb{Z}$  is a principal ideal domain, the above shows that every ideal of  $\mathbb{Z} \oplus \mathbb{Z}$  is principal.

(ii) Every ideal of  $\mathbb{Z}/(4)$  is the image of an ideal of  $\mathbb{Z}$ , hence is principal.

(iii) The Chinese remainder theorem implies that  $\frac{\mathbb{Z}}{(6)}[x] \approx \frac{\mathbb{Z}}{(2)}[x] \oplus \frac{\mathbb{Z}}{(3)}[x]$ . Since each of  $\frac{\mathbb{Z}}{(2)}[x]$  and  $\frac{\mathbb{Z}}{(3)}[x]$  is a principal ideal domain, it follows that every ideal of  $\frac{\mathbb{Z}}{(6)}[x]$  is principal.

(iv) Suppose the ideal  $(2, x)$  of  $\mathbb{Z}/(4)[x]$  is principal, then so is its image in the ring  $\mathbb{Z}[x]/(4, x^2)$ . Consequently there exist  $a, b \in \mathbb{Z}/(4)$  with  $(2, x) = (a + bx)$  in  $\mathbb{Z}[x]/(4, x^2)$ . Examining this modulo  $x$  and modulo 2, we see that  $a = 2$  and  $b = \pm 1$ , i.e., without loss of generality, we have  $(2, x) = (2 + x)$  in  $\mathbb{Z}[x]/(4, x^2)$ . In particular,  $2 = (2 + x)(c + dx)$  and so  $2c = 2$  and  $c + 2d = 0$  in  $\mathbb{Z}/(4)$ . But this gives a contradiction, so  $(2, x)$  is not a principal ideal of  $\mathbb{Z}/(4)[x]$ .

6. Let  $f(x) \in \mathbb{Z}[x]$  be a monic polynomial. If  $f(a) = 0$  for some  $a \in \mathbb{Q}$ , prove that  $a \in \mathbb{Z}$ .

**Solution:** If  $a \neq 0$  then, after perhaps factoring out a power of  $x$ , we may assume that  $f(x)$  has a nonzero constant term, i.e.,

$$f(x) = x^k + r_1x^{k-1} + \cdots + r_k \quad \text{where } r_i \in \mathbb{Z} \quad \text{and } r_n \neq 0.$$

Let  $a = m/n$  for nonzero relatively prime integers  $m, n$  with  $n \geq 1$ . After clearing denominators,  $f(a) = 0$  implies that

$$m^k + r_1m^{k-1}n + \cdots + r_kn^k.$$

But then any prime which divides  $n$  also divides  $m$ , so  $n = 1$ .

7. Let  $M$  be a  $3 \times 3$  matrix with complex entries. If  $M^3$  is the identity matrix, what are the possibilities for the Jordan canonical form of  $M$ ?

**Solution:** The minimal polynomial of  $M$  divides  $f(t) = t^3 - 1$ , which factors as

$$f(t) = (t - 1)(t - \omega)(t - \omega^2) \quad \text{where } \omega = e^{2\pi i/3}.$$

Each of the invariants  $q_i(t)$  of  $M$  must divide  $f(t)$ , and so each  $q_i(t)$  has distinct roots. Consequently the Jordan canonical form of  $M$  is a  $3 \times 3$  diagonal matrix, with the elements occurring along the diagonal being some—or all—of the elements  $1, \omega, \omega^2$ .

8. Let  $M$  be a  $3 \times 3$  matrix with integer entries and  $\det(M) = -1$ . Assume that every real eigenvalue of  $M$  is rational. What are the possibilities for the minimal polynomial and Jordan canonical form of  $M$ ?

**Solution:** The characteristic polynomial of  $M$  is  $t^3 + at^2 + bt + 1 \in \mathbb{Z}[t]$ , whose only integer roots are  $\pm 1$ . If all eigenvalues are real, then they are all rational by hypothesis, and hence are all integers by Problem 6. The possible eigenvalues in this case are  $-1, 1, 1$  and  $-1, -1, -1$ , and the possible minimal polynomials for  $M$  are

$$(t + 1)(t - 1), \quad (t + 1)(t - 1)^2, \quad (t + 1), \quad (t + 1)^2, \quad (t + 1)^3.$$

Up to permutation of the Jordan blocks, the possible Jordan canonical forms of  $M$  are

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}.$$

If  $\lambda$  is a complex eigenvalue, then so is its complex conjugate  $\bar{\lambda}$ . The third eigenvalue is the real number, hence integer,  $-1/|\lambda|^2$ . The only possible value of this is  $-1$ , so we have three distinct eigenvalues  $-1, \lambda, \bar{\lambda}$ . The minimal polynomial is  $(t + 1)(t - \lambda)(t - \bar{\lambda})$  where  $\lambda$  is a complex number with  $|\lambda| = 1$ , and the Jordan canonical form, up to permutation of the diagonal elements, is

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \bar{\lambda} \end{pmatrix}.$$