

## Solutions to Chapter 2

**Solution to Exercise 2.26.** Suppose for a contradiction that  $R = N_1 \oplus N_2$  where  $N_1, N_2$  are nonzero ideals of  $R$ . If  $a \in N_1$  and  $b \in N_2$  are any nonzero elements, then  $ab$  is a nonzero element of  $N_1 \cap N_2$ , which gives the contradiction.

Note that we only used here the fact that  $R$  was an integral domain, not that it was a PID. If  $R$  is not an integral domain, it can be decomposable as a module over itself: for example, Exercise 1.108 showed that  $\mathbb{Z}_6$  is decomposable as a  $\mathbb{Z}$ -module, and the decomposition  $\mathbb{Z}_6 = \{0, 3\} \oplus \{0, 2, 4\}$  is equally valid in the category of  $\mathbb{Z}_6$ -modules.

**Solution to Exercise 2.27.** Let  $M$  be a finitely-generated  $R$ -module. Choose a generating set  $\{x_1, \dots, x_n\}$  of  $M$ ; as seen in Proposition 1.71, this gives rise to a surjective  $R$ -module homomorphism  $\varphi : R^n \rightarrow M$ . If  $N$  is any submodule of  $M$ , then  $\varphi^{-1}(N)$  is a submodule of  $R^n$ . But by Theorem 2.20,  $\varphi^{-1}(N)$  must have some finite basis  $\{y_1, \dots, y_m\}$  where  $m \leq n$ ; since  $\varphi$  is surjective, we have  $N = \varphi(\varphi^{-1}(N))$ , so  $N$  is generated by  $\{\varphi(y_1), \dots, \varphi(y_m)\}$ . So we have shown that every submodule of a finitely-generated  $R$ -module is finitely-generated. (As observed in Exercise 1.60, this is not true for the ring  $F[x_1, x_2, \dots]$ . The commutative rings  $R$  for which it is true are called “noetherian” after the German algebraist Emmy Noether.)

**Solution to Exercise 2.29.** Let  $N$  be the ideal of  $R$  generated by  $x$  and  $y$ ; as noted in Example 2.9,  $N$  is not principal.  $N$  is certainly a finitely-generated torsion-free  $R$ -module, but it is not free, for the reason mentioned in Exercise 1.81: a basis of  $N$  would have to consist of at least two elements,

but any two nonzero elements  $r_1, r_2 \in N$  satisfy the linear dependence  $r_2r_1 + (-r_1)r_2 = 0$ .

**Solution to Exercise 2.62.**

- (i) According to the procedures given in Section 2.3, we should consider the matrix  $\begin{pmatrix} 2 & 3 & 4 \\ 1 & -1 & -5 \\ -1 & 1 & 3 \end{pmatrix}$ . Its determinant is 10, which implies that its columns are linearly independent, so the set itself is an acceptable basis of the submodule in question. (Note that this submodule is not the whole of  $\mathbb{Z}^3$ : for that, the determinant would have had to be  $\pm 1$ ). But supposing that we don't know the determinant but instead want to put the matrix in column-echelon form, the first step is to right-multiply by  $\begin{pmatrix} -1 & -3 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ , which produces  $\begin{pmatrix} 1 & 0 & 4 \\ -2 & -5 & -5 \\ 2 & 5 & 3 \end{pmatrix}$ . Applying the column operation  $C_3 \rightarrow C_3 - 4C_1$ , this becomes  $\begin{pmatrix} 1 & 0 & 0 \\ -2 & -5 & -5 \\ 2 & 5 & -5 \end{pmatrix}$ . We then right-multiply by  $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -3 \\ 0 & 2 & -5 \end{pmatrix}$ , which produces  $\begin{pmatrix} 1 & 0 & 0 \\ -2 & 1 & 0 \\ 2 & -5 & 10 \end{pmatrix}$ . So another basis for the submodule is  $\{(1, -2, 2), (0, 1, -5), (0, 0, 10)\}$ .
- (ii) Right-multiplying  $\begin{pmatrix} x & x+1 \\ x^2-x & x^2-1 \end{pmatrix}$  by the invertible matrix  $\begin{pmatrix} -1 & -x^{-1} \\ 1 & x \end{pmatrix}$ , we get  $\begin{pmatrix} 1 & 0 \\ x-1 & 0 \end{pmatrix}$ , which implies that the submodule has rank 1 and basis  $\{(1, x-1)\}$ .
- (iii) We have a chain of column equivalences:

$$\begin{pmatrix} 2x-1 & x & x \\ x & x^2 & x \\ 3x-1 & -x^2+3x & x+1 \end{pmatrix} \xrightarrow{C_1 \rightarrow C_1 - 2C_3} \begin{pmatrix} -1 & x & x \\ -x & x^2 & x \\ x-3 & -x^2+3x & x+1 \end{pmatrix} \xrightarrow{C_2 \rightarrow C_2 + xC_1, C_3 \rightarrow C_3 + xC_1} \begin{pmatrix} -1 & 0 & 0 \\ -x & 0 & x-x^2 \\ x-3 & 0 & x^2-2x+1 \end{pmatrix}.$$

We could obviously put the latter matrix in column-echelon form by swapping the second and third columns. So a basis is

$$\{(-1, -x, x-3), (0, x-x^2, x^2-2x+1)\}.$$

**Solution to Exercise 2.63.**

- (i) Clearly  $x + xy + N = (1 + y)(x + N)$  belongs to the ideal of  $R/N$  generated by  $x + N$ , and  $x + N = x - xy^2 + N = (1 - y)(x + xy + N)$  belongs to the ideal of  $R/N$  generated by  $x + xy + N$ , so  $x + N$  and  $x + xy + N$  generate the same ideal of  $R/N$ . We must now find which elements of  $R/N$  are invertible. But if  $p + N$  is invertible in  $R/N$ , its image in the quotient ring  $R/Ry \cong F[x]$  must also be invertible, which means that the constant term of  $p$  is nonzero and  $p$  contains no  $x^i$  terms for  $i \geq 1$ . Similarly  $p$  contains no  $y^i$  terms for  $i \geq 1$ , so  $p + N$  must be of the form  $a + bxy + N$  where  $a, b \in F$  and  $a$  is nonzero. Conversely, any element of this form is invertible, because

$$(a + bxy + N)(a^{-1} - a^{-2}bxy + N) = 1 - a^{-2}b^2x^2y^2 + N = 1 + N.$$

However,  $(x + N)(a + bxy + N) = ax + bx^2y + N = ax + N$  cannot equal  $x + xy + N$ , so  $x + xy + N$  cannot be obtained from  $x + N$  by multiplying by an invertible element of  $R/N$ . (This phenomenon of having non-associate elements generating the same ideal couldn't happen in an integral domain. It can also be shown that it can't happen in a ring which is a product of quotients of PIDs, which is why this example had to be so far-fetched.)

- (ii) Clearly  $R\{x + xy, y^2\} \subseteq R\{x, y^2\}$ , and the other direction follows from  $x = (1 - y)(x + xy) + xy^2$ . Suppose that  $Y = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \text{Mat}_2(R)$  was invertible and satisfied  $\begin{pmatrix} x & xy \\ y^2 & y^2 \end{pmatrix} = \begin{pmatrix} x & y^2 \end{pmatrix} Y$ . Then  $\det(Y)$  is an invertible element of  $R$ ; in other words,  $ps - qr$  is a nonzero constant. The matrix equation is equivalent to

$$\begin{aligned} x + xy &= xp + y^2r, \\ y^2 &= xq + y^2s. \end{aligned}$$

The second of these equations forces  $q = y^2q'$ ,  $s = 1 - xq'$  for some  $q' \in R$ . The first forces  $p = 1 + y + y^2p'$ ,  $r = -xp'$  for some  $p' \in R$ . We then have

$$ps - qr = (1 + y + y^2p')(1 - xq') + xy^2p'q' = 1 + y + y^2p' - xq' - xyq',$$

which clearly has a nonzero  $y$  term, giving us the desired contradiction. (As noted in Remark 2.61, this phenomenon can't happen in a principal ideal domain.)

**Solution to Exercise 2.92.**

- (i) If  $(a)$  and  $(b)$  are  $1 \times 1$  matrices over  $R$ , then they are equivalent if and only if  $b = xay$  for some invertible  $x, y \in R$ ; in other words, if and only if  $a$  and  $b$  are associates in  $R$ . So an example is  $A = (1)$  and  $B = (2)$ , since 1 and 2 are associates in  $\mathbb{Q}$  but not in  $\mathbb{Z}$ .
- (ii) This time there is no hope of such a simple example, because for  $1 \times 1$  (or, more generally,  $1 \times m$ ) matrices there is no difference between being column-equivalent over  $\mathbb{Z}$  and being equivalent over  $\mathbb{Z}$ . It is also easy to see that there cannot be an example using  $n \times 1$  matrices, so the smallest possible size is  $2 \times 2$ . One example is

$$A = \begin{pmatrix} 2 & 5 \\ 0 & 3 \end{pmatrix}, B = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}.$$

These are equivalent over  $\mathbb{Z}$  because  $B$  can be obtained from  $A$  by applying the column operation  $C_2 \rightarrow C_2 - C_1$  and the row operation  $R_1 \rightarrow R_1 - R_2$ . They are also column-equivalent over  $\mathbb{Q}$  because  $B$  can be obtained from  $A$  by the column operation  $C_2 \rightarrow C_2 - \frac{5}{2}C_1$ . But  $A$  and  $B$  are not column-equivalent over  $\mathbb{Z}$ , i.e. there is no invertible integer matrix  $Y$  such that  $A = BY$ ; this follows from the fact that  $B^{-1}A = \begin{pmatrix} 1 & \frac{5}{2} \\ 0 & 1 \end{pmatrix}$  has a non-integer entry.

- (iii) Since  $A$  and  $B$  must have the same determinant, we need the determinant to have a repeated prime factor so that there is scope for  $A$  and  $B$  to have different invariant factors. One example is

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 5 \end{pmatrix}, B = \begin{pmatrix} -2 & -2 \\ 10 & 8 \end{pmatrix}.$$

These both have determinant 4 and trace 6, so they have the same characteristic polynomial, namely  $x^2 - 6x + 4$ . As we will see later, the fact that this polynomial is irreducible over  $\mathbb{Q}$  means that all matrices which have it as their characteristic polynomial are conjugate over  $\mathbb{Q}$ ; but in any case, we can see directly that  $B = X^{-1}AX$  where  $X = \begin{pmatrix} 10 & 3 \\ 0 & 1 \end{pmatrix}$ . (There are many other choices of conjugating matrix; in this choice  $X$  does have integer entries, but  $X^{-1}$  doesn't.) However,  $A$  and  $B$  are not equivalent over  $\mathbb{Z}$ , because  $A$  has invariant factors 1, 4 while  $B$  has invariant factors 2, 2.

**Solution to Exercise 2.93.**

- (i) We have  $a_1 = \gcd(6, 15) = 3$  and  $a_1 a_2 = 6 \times 15 = 90$ . So the invariant factors are 3 and 30. Alternatively, apply the method of ordering the prime factors as in Proposition 2.87.
- (ii) Clearing the first row with column operations gives  $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 2 & -1 & -2 & -3 \end{pmatrix}$ . We can then eliminate the 2 with  $R_2 \rightarrow R_2 - 2R_1$  and then the  $-2$  and the  $-3$  with column operations to get the normal-form matrix  $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$ . So the invariant factors are 1 and 1. In terms of minors, this expresses the fact that the  $2 \times 2$  minors have no common factor (indeed, the determinant of the left-hand  $2 \times 2$  submatrix is  $-1$ ).
- (iii) Algorithm 2.76 gives that this matrix is equivalent to  $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 15 \\ 0 & 0 & 20 \end{pmatrix}$ . At this point it is best to diverge from the algorithm (which does something drastic since  $2 \nmid 15$ ), and consider the minors of the simpler matrix. The gcd of the entries is obviously 1, so  $a_1 = 1$ ; the gcd of the  $3 \times 3$  minors is 10, so  $a_1 a_2 a_3 = 10$ ; and then the divisibility requirement shows that  $a_2 = 1$ ,  $a_3 = 10$ .
- (iv) The gcd of the entries is 1 and the determinant is 12, so the invariant factors must be  $1, a_2, 12/a_2$  where  $a_2^2 \mid 12$ . The only possibilities for  $a_2$  are 1 and 2, so we just need to determine whether all the  $2 \times 2$  minors are even. But the second row is all even, so any submatrix involving that will have even determinant; and any  $2 \times 2$  submatrix avoiding the second row will have all four entries odd, hence even determinant. So the invariant factors are 1, 2, 6. (Of course you can also get this via row and column operations.)

**Solution to Exercise 2.94.**

- (i) Following the method given by Proposition 2.87 for finding invariant factors of a diagonal matrix, we find the irreducible factorizations:

$$\begin{aligned} 1 + x &= x^0(1 - x)^0(1 + x)^1, \\ x &= x^1(1 - x)^0(1 + x)^0, \\ 1 - x^2 &= x^0(1 - x)^1(1 + x)^1. \end{aligned}$$

It follows that the invariant factors are  $1, 1 + x, x(1 - x)(1 + x)$ .

- (ii) We can see that the first invariant factor  $a_1$  is 1 because the entries have no common factor. Calculating some  $2 \times 2$  minors reveals that they have no common factor either, so  $a_1 a_2$  is also 1. The determinant of the whole matrix is  $-3x^3 + 4x^2 - 3x$ , so the invariant factors are  $1, 1, -3x^3 + 4x^2 - 3x$ . The fact that the determinant has no repeated irreducible factors forces the first two invariant factors to be 1, so the calculation of minors was not actually required. (Of course you can also find the invariant factors via row and column operations.)

**Solution to Exercise 2.95.** The gcd of the entries is quickly seen to be  $1 + i$  (which divides  $2 = -i(1 + i)^2$ ). There are three  $2 \times 2$  submatrices to consider, and their determinants are  $12, 2 - 2i$ , and  $4$ . The gcd of these is  $2 - 2i = (1 + i)^3$ . So the invariant factors are  $1 + i$  and  $(1 + i)^2$ .

**Solution to Exercise 2.96.**

- (i) We know that  $XAY = \text{diag}(a_1, \dots, a_{\min\{n,m\}})$  for some invertible matrices  $X, Y$ . So

$$X(rA)Y = rXAY = \text{diag}(ra_1, \dots, ra_{\min\{n,m\}}),$$

and we also have  $ra_1 \mid ra_2 \mid \dots \mid ra_{\min\{n,m\}}$ , proving the claim. Alternatively, one can use the fact that the  $k \times k$  minors of  $rA$  are  $r^k$  times the  $k \times k$  minors of  $A$ .

- (ii) Transposing the equation  $XAY = \text{diag}(a_1, \dots, a_{\min\{n,m\}})$ , we obtain

$$Y^t A^t X^t = \text{diag}(a_1, \dots, a_{\min\{n,m\}})^t = \text{diag}(a_1, \dots, a_{\min\{n,m\}}).$$

Now the fact that  $X$  and  $Y$  are invertible implies that  $X^t$  and  $Y^t$  are also (for example, transposing  $XX^{-1} = 1_n$  gives  $(X^{-1})^t X^t = 1_n$ ). So  $A^t$  is equivalent to  $\text{diag}(a_1, \dots, a_{\min\{n,m\}})$ , and hence has the same invariant factors as  $A$ .

- (iii) This is a bit of a trick question: if  $A$  is invertible, then  $\det(A)$  is a unit in  $R$ , so its invariant factors are all units in  $R$ , and we may as well call them all 1. (Conversely, a square matrix whose invariant factors are all units has determinant which is a unit and is therefore invertible.) So the answer to the question is that the invariant factors of  $A^{-1}$  (which of course is also invertible!) are all 1.

- (iv) It is a fact that for any  $A, B \in \text{Mat}_n(R)$ ,  $\text{adj}(AB) = (\text{adj } B)(\text{adj } A)$ . Thanks to the assumption of nonzero determinant, we only need the case of this where  $\det(A)$  and  $\det(B)$  are nonzero; this case follows from the equation

$$\begin{aligned} AB \text{adj}(AB) &= \det(AB)1_n = \det(B) \det(A)1_n \\ &= \det(B)A(\text{adj } A) = A(\det(B)1_n)(\text{adj } A) \\ &= AB(\text{adj } B)(\text{adj } A), \end{aligned}$$

since the columns of  $AB$  must be linearly independent for  $\det(AB) \neq 0$  to hold, and that means we can cancel  $AB$  from the left. It follows that if  $X \in \text{Mat}_n(R)$  is invertible, then so is  $\text{adj } X$ . Taking adjugates of the equation  $XAY = \text{diag}(a_1, \dots, a_n)$ , we deduce that

$$\begin{aligned} (\text{adj } Y)(\text{adj } A)(\text{adj } X) &= \text{adj}(\text{diag}(a_1, \dots, a_n)) \\ &= \text{diag}(a_2 a_3 \cdots a_n, a_1 a_3 \cdots a_n, \dots, a_1 a_2 \cdots a_{n-1}). \end{aligned}$$

The latter diagonal matrix is not in normal form, but we can simply reverse the order of the rows and columns to make it so. So the answer is that the invariant factors of  $\text{adj } A$  are  $a_1 a_2 \cdots a_{n-1}, \dots, a_2 a_3 \cdots a_n$ .

### Solution to Exercise 2.97.

- (i) There are plenty of examples to demonstrate this. One could consider  $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$  and  $B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ , so that  $a_1 = b_1 = 1$ ,  $a_2 = b_2 = 0$ , whereas  $AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$  has invariant factors  $0, 0$ .
- (ii) Recall from Exercise 2.96(ii) that the invariant factors of the transpose matrix  $A^t$  are the same as those of  $A$ . Since  $(AB)^t = B^t A^t$ , taking transpose of all matrices interchanges the role of  $A$  and  $B$  in the question. So it suffices to show that  $a_k \mid c_k$  for  $k = 1, 2, \dots, n$ .

Write  $D_A, D_B, D_C$  for  $\text{diag}(a_1, a_2, \dots, a_n)$  etc. Then  $A = X_A D_A Y_A$  and  $B = X_B D_B Y_B$  for some invertible  $X_A, X_B, Y_A, Y_B \in \text{Mat}_n(R)$ , so

$$D_A Y_A X_B D_B = X_A^{-1} A B Y_B^{-1} \text{ is equivalent to } D_C.$$

All we need to take away from this is that  $c_1, \dots, c_n$  are the invariant factors of  $D_A M$  for some  $M = (m_{ij}) \in \text{Mat}_n(R)$ . There are now (at least) three ways to proceed.

**Method 1.** For  $1 \leq k \leq n$ , consider any  $k \times k$  minor of  $D_A M$ , say the determinant of the submatrix formed using rows  $i_1, \dots, i_k$  and columns  $j_1, \dots, j_k$ . By expanding this determinant along its final row, we see that it is a multiple of  $a_{i_k}$  times the gcd of all  $(k-1) \times (k-1)$  minors of  $D_A M$ . (To make this true when  $k = 1$ , we need the convention that the determinant of the unique  $0 \times 0$  matrix is 1.) We know that this gcd is  $c_1 \cdots c_{k-1}$ . Also  $a_{i_k}$  is a multiple of  $a_k$  (since  $i_k \geq k$ ). So  $c_1 \cdots c_{k-1} a_k$  divides every  $k \times k$  minor of  $D_A M$ , and hence divides their gcd, which is  $c_1 \cdots c_k$ . So we have shown that

$$c_1 \cdots c_{k-1} a_k \mid c_1 \cdots c_{k-1} c_k.$$

If  $c_1 \cdots c_{k-1} \neq 0$ , we can conclude that  $a_k \mid c_k$ . If  $c_1 \cdots c_{k-1} = 0$ , then we must have  $c_i = 0$  for some  $1 \leq i \leq k-1$ , and then the divisibility constraints imply that  $c_k = 0$ , so  $a_k \mid c_k$  in this case also.

**Method 2.** We have  $D_A M = X D_C Y$  for some invertible  $X, Y \in \text{Mat}_n(R)$ . Renaming  $M$  as  $MY$ , we can get rid of  $Y$ , and thus get  $D_A M = X D_C$ , which says that  $a_i m_{ij} = x_{ij} c_j$  for all  $i, j$ . Now suppose for a contradiction that  $a_k \nmid c_k$ . Then there must be an irreducible element  $p \in R$  and a positive integer  $\ell$  such that  $p^\ell \mid a_k$  but  $p^\ell \nmid c_k$ . Since  $a_k \mid a_i$  for all  $i \geq k$ , we have  $p^\ell \mid x_{ij} c_j$  for all  $i \geq k$ . Since  $c_j \mid c_k$  for all  $j \leq k$ , we have  $p^\ell \nmid c_j$  for all  $j \leq k$ , and we conclude that  $p \mid x_{ij}$  for all  $i \geq k, j \leq k$ . But every term of  $\det(X)$  must contain some such  $x_{ij}$ , so this would mean  $p \mid \det(X)$ , which is impossible because  $\det(X)$  is a unit.

**Method 3.** The matrix  $D_A M$  has the property we'll call Property K: that  $a_k$  divides the  $k$ th row, for  $k = 1, \dots, n$ . It suffices to show that we can carry out invertible row and column operations which will bring the matrix into normal form while maintaining Property K all the time; at the end of the procedure,  $a_k$  will divide the  $k$ th entry of the diagonal, which will be  $c_k$ . Any column operations clearly maintain Property K, as do the operations of multiplying a row by a unit. A row operation  $R_i \rightarrow R_i + cR_j$  for  $i < j$  also maintains Property K, because  $a_i \mid a_j$ . A row operation  $R_i \rightarrow R_i + cR_j$  for  $i > j$  usually won't maintain Property K, but it clearly will in the special case that  $R_j$  is zero except for the  $(j, \ell)$  entry and the new  $R_i$  has a zero in the  $(i, \ell)$  entry. Similarly, a row swap usually won't maintain Property K, but it clearly will in the special case that the row with the smaller number is zero. It is easy to make a slight modification of Algorithm 2.76 so that we only ever use these special cases of the last two kinds of operations.

**Solution to Exercise 2.112.** The presentation matrix  $A$  in this case is the  $2 \times 1$  matrix  $\begin{pmatrix} a \\ b \end{pmatrix}$ . The main point is that the sole invariant factor of this matrix is  $d$  (the gcd of the entries). We now have three cases.

- If  $d = 0$  (i.e.  $a = b = 0$ ), the module  $Rx + Ry$  has no torsion invariants, and its rank equals  $2 - \text{rk}(A) = 2$ , so it is isomorphic to  $R \oplus R \cong R/R0 \oplus R$  as claimed.
- If  $d$  is a unit, the module  $Rx + Ry$  has no torsion invariants, and its rank equals  $2 - \text{rk}(A) = 1$ , so it is isomorphic to  $R \cong R/R1 \oplus R$  as claimed.
- If  $d$  a nonzero non-unit, the module  $Rx + Ry$  has sole torsion invariant  $d$ , and its rank equals  $2 - \text{rk}(A) = 1$ , so it is isomorphic to  $R/Rd \oplus R$ .

**Solution to Exercise 2.113.**

- (i) Clearly  $\text{rk}(\mathbb{Z}_n) = 0$  and the sole torsion invariant is  $n$  (except if  $n = 1$ , in which case there are no torsion invariants and the module is  $\{0\}$ ).
- (ii) Again we are dealing with a torsion module, so the rank is 0. The torsion invariants can be obtained by factorizing 20, 140, and 108 and then ordering the powers of each prime: they are  $2^2 = 4$ ,  $2^2 \times 5 = 20$ , and  $2^2 \times 3^3 \times 5 \times 7 = 3780$ . (That is,  $M \cong \mathbb{Z}_4 \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}_{3780}$ .)
- (iii) The presentation matrix is  $\begin{pmatrix} 2 & 3 & 4 \\ 1 & -1 & -5 \\ -1 & 1 & 3 \end{pmatrix}$ . From the calculations in Exercise 2.62(i), it is easy to see that the invariant factors of this matrix are 1, 1, 10. So  $M$  has rank  $3 - 3 = 0$ , and sole torsion invariant 10. (That is,  $M \cong \mathbb{Z}_{10}$ .)
- (iv) The field  $\mathbb{Z}_p$  is free of rank 1 as a module over itself, and there are no torsion invariants.
- (v) We have  $M \cong F[x]/F[x](x - 3)$ , so the rank is 0 and the sole torsion invariant is  $x - 3$ .
- (vi) We have  $M \cong F[x]/F[x]x^2$ , so the rank is 0 and the sole torsion invariant is  $x^2$ .

**Solution to Exercise 2.114.** By definition, the invariant factors of  $M$  in  $R^n$  are all 1 if and only if there is a basis  $\{f_1, \dots, f_n\}$  of  $R^n$  such that  $\{f_1, \dots, f_r\}$  is a basis of  $M$  for some  $0 \leq r \leq n$ . If this is the case, then it is easy to see that the submodule generated by the remaining basis elements, namely  $R\{f_{r+1}, \dots, f_n\}$ , is complementary to  $M$  in  $R^n$ ; moreover, the images  $f_{r+1} + M, \dots, f_n + M$  form a basis for  $R^n/M$ . So (1) implies (2) and (3). If we assume the existence of a complementary submodule  $M'$ , then knowing that both  $M$  and  $M'$  must have finite bases, we can take the union of these to get a basis of  $M \oplus M' = R^n$ ; also,  $R^n/M$  is isomorphic to  $M'$  and hence free. So (2) implies (1) and (3). We saw that (3) implies (2) in Exercise 1.115. This gives more than enough implications to prove the result.

**Solution to Exercise 2.115.** First consider the special case where  $M$  is a free module, i.e.  $M$  is isomorphic to  $R^n$  for some  $n$ . By Theorem 2.98, there is some basis  $\{f_1, \dots, f_n\}$  of  $M$  such that  $\{a_1 f_1, \dots, a_r f_r\}$  is a basis of  $N$ , where  $r = \text{rk}(N)$  and  $a_1, \dots, a_r$  are the invariant factors of  $N$  in  $M$ . As seen in the proof of Theorem 2.102, it then follows that  $M/N \cong R/Ra_1 \oplus \dots \oplus R/Ra_r \oplus R \oplus \dots \oplus R$ , where the number of copies of  $R$  is  $n - r$ . Hence  $\text{rk}(M/N) = n - r = \text{rk}(M) - \text{rk}(N)$  as required.

Now return to the general case where  $M$  is not necessarily free. Since  $M$  is finitely-generated, there is a surjective  $R$ -module homomorphism  $\varphi : R^n \rightarrow M$  for some  $n$ . Let  $N' = \varphi^{-1}(N)$ , a submodule of  $R^n$  containing  $\ker(\varphi)$ ; since  $\varphi$  is surjective, the restriction  $\varphi : N' \rightarrow N$  is also surjective. Then by the First Isomorphism Theorem we have  $M \cong R^n / \ker(\varphi)$  and  $N \cong N' / \ker(\varphi)$ , and by the Third Isomorphism Theorem we have  $M/N \cong R^n / N'$ . By the special case we have already proved, these isomorphisms tell us that

$$\begin{aligned}\text{rk}(M) &= n - \text{rk}(\ker(\varphi)), \\ \text{rk}(N) &= \text{rk}(N') - \text{rk}(\ker(\varphi)), \\ \text{rk}(M/N) &= n - \text{rk}(N').\end{aligned}$$

From these equations it obviously follows that  $\text{rk}(M/N) = \text{rk}(M) - \text{rk}(N)$ .

**Solution to Exercise 2.127.** In part (i), the primary invariants are the prime powers in the factorization of  $n$ . In part (ii), the primary invariants are the prime-power factors of the torsion invariants 4, 20, 3780 (or equivalently

of the original numbers 20, 140, 108): namely,  $2^2$ ,  $2^2$ ,  $2^2$ ,  $3^3$ , 5, 5, and 7. In part (iii), the primary invariants are 2 and 5. In part (iv) there are no primary invariants. In part (v) the sole primary invariant is  $x - 3$ , and in part (vi) the sole primary invariant is  $x^2$ .

**Solution to Exercise 2.128.**

- (i) Obviously  $G^{[k]}$  contains the identity and is closed under taking inverses. If  $G$  is abelian and  $g, h \in G^{[k]}$ , then  $(gh)^{p^k} = g^{p^k} h^{p^k} = 1$ , so  $gh \in G^{[k]}$  also. This shows that  $G^{[k]}$  is a subgroup.
- (ii) Let  $G$  be the group of symmetries of a square, a group of order  $8 = 2^3$  consisting of four reflections and four rotations (counting the identity as a rotation through 0 degrees). If  $g$  is a reflection about a line joining two corners and  $h$  is a reflection about a line joining the midpoints of opposite sides, then  $g^2 = h^2 = 1$ , so  $g, h \in G^{[1]}$ . However,  $gh$  is then a rotation through 90 degrees, so it has order 4 rather than 2, and  $gh \notin G^{[1]}$ .
- (iii) Note that  $C_{p^m}^{[k]}$  is all of  $C_{p^m}$  if  $k \geq m$ , and otherwise is a subgroup isomorphic to  $C_{p^k}$ . So we have

$$\begin{aligned} |G^{[k]}| &= |C_{p^{n_1}}^{[k]}| \times |C_{p^{n_2}}^{[k]}| \times \cdots \times |C_{p^{n_s}}^{[k]}| \\ &= p^{\min\{k, n_1\}} \times p^{\min\{k, n_2\}} \times \cdots \times p^{\min\{k, n_s\}} \\ &= p^{\min\{k, n_1\} + \min\{k, n_2\} + \cdots + \min\{k, n_s\}}. \end{aligned}$$

If we now replace  $k$  by  $k + 1$ , the terms in the exponent which will change are those  $\min\{k, n_i\}$  where  $k < n_i$ ; these will each increase by 1. So knowing all the numbers  $|G^{[k]}|$  tells us, for every  $k = 0, 1, \dots, n$ , how many of the  $n_i$ 's are strictly greater than  $k$ . The amount by which this number decreases as  $k - 1$  is replaced by  $k$  tells us how many of the  $n_i$ 's are equal to  $k$ , and that determines the sequence of  $n_i$ 's.