Rings and Modules Problems

1. Rings and fields

Q1: Which of the following are commutative rings?

- R_0 is the set of polynomials $f(x) \in \mathbb{R}[x]$ such that $f(-x) = f(x)$.
- R_1 is the set of polynomials $f(x) \in \mathbb{R}[x]$ such that $f(-x) = -f(x)$.
- R_2 is the set of 2×2 matrices over $\mathbb{R}$, with the usual definition of matrix multiplication.
- R_3 is the set of 2×2 matrices over $\mathbb{R}$, with multiplication given by the definition
$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) = \left(\begin{smallmatrix} aa' & bb' \\ cc' & dd' \end{smallmatrix}\right).$$
- R_4 is the set of vectors in $\mathbb{R}^3$, with multiplication given by the cross product:
$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} \times \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} yz' - y'z \\ zx' - z'x \\ xy' - x'y \end{pmatrix}.$$

Solution:

- R_0 is a ring. The main point is to observe that R_0 is closed under addition and multiplication, because if $f(-x) = f(x)$ and $g(-x) = g(x)$ then
$$(f+g)(-x) = f(-x) + g(-x) = f(x) + g(x) = (f+g)(x)$$
$$fg(-x) = f(-x)g(-x) = f(x)g(x) = fg(x).$$
- R_1 is not a ring, because it is not closed under multiplication: if f and g lie in R_1 then
$$fg(-x) = f(-x)g(-x) = (-f(x))(-g(x)) = +fg(x) \neq -fg(x),$$
so $fg \notin R_1$ (except in trivial cases where $fg = 0$).
- R_2 is not a commutative ring, because matrix multiplication is not commutative in general. For example, if we take $a = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ and $b = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ then $ab = b$ and $ba = 0$ so $ab \neq ba$. All the other axioms are satisfied, however.
- R_3 is a ring. The additive identity is the zero matrix, and the multiplicative identity is the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$.
- R_4 is not a ring. Firstly, it is not commutative, because $b \times a = -a \times b$. It is not even associative, because
$$a \times (b \times c) = (a.c)b - (a.b)c$$
$$(a \times b) \times c = (a.c)b - (b.c)a.$$
There is also no multiplicative identity: if there were, then we would have $1 \times 1 = 1$, but $a \times a$ is always zero for any vector a. (R_3 is in fact an example of a *Lie algebra*; these are rather different from rings, but also very important.)

Q2: Choose two typical elements a and b of the ring $\mathbb{Z}_{(5)}$. Find $a+b$ and ab and check that they lie in $\mathbb{Z}_{(5)}$. Repeat this for the rings $\mathbb{Z}[i]$, $\mathbb{Q}[x,y]$ and $\mathbb{Z}_{12}$.

Solution:

(a) In $\mathbb{Z}_{(5)}$ we could take $a = 3/4$ and $b = 6/7$; these both lie in $\mathbb{Z}_{(5)}$ because 4 and 7 are not divisible by 5. We have $a+b = 45/28$ and $ab = 18/28 = 9/14$. These both lie in $\mathbb{Z}_{(5)}$ because 28 and 14 are not divisible by 5.

(b) In $\mathbb{Z}[i]$ we could take $a = 2+3i$ and $b = 4-5i$. We then have $a+b = 6-2i$ and $ab = 23+2i$; both of these clearly also lie in $\mathbb{Z}[i]$.

(c) In $\mathbb{Q}[x,y]$ we could take $a = (x+y)/2$ and $b = (x-y)/2$. Then $a+b = x$ and $ab = (x^2-y^2)/4$, so $a+b$ and ab are again elements of $\mathbb{Q}[x,y]$.

(d) In $\mathbb{Z}_{12}$ we could take $a = \overline{3}$ and $b = \overline{4}$, so $a + b = \overline{7} = \overline{-5}$ and $ab = \overline{12} = \overline{0}$.

Q3: Let R be the set of rational numbers that can be written in the form a/b, where b is not divisible by 6. (We would call this $\mathbb{Z}_{(6)}$ if 6 were prime, which of course it isn't). Prove that R is *not* a subring of $\mathbb{Q}$.

Solution: Put $a = 1/2$ and $b = -1/3$. Then $a, b \in R$ but $a+b = 1/6 \notin R$ and $ab = -1/6 \notin R$, so R is not closed under addition or multiplication.

Q4: Let K be a field; prove that K is an integral domain.

Solution: Let a and b be nonzero elements of K; we must prove that $ab \neq 0$. As K is a field, we know that a and b are invertible, so we can find elements $c, d \in K$ with $ac = 1$ and $bd = 1$. It follows that $abcd = 1$. If ab were zero we would also have $abcd = 0$, so 1 would be equal to 0, contradicting the definition of a field. We must thus have $ab \neq 0$ as required.

Q5: Let X be a set. Let R be the set of all subsets of X, and define addition and multiplication of subsets as follows.

$$\begin{aligned} A + B &= (A \cup B) \setminus (A \cap B) \\ &= \{x \in X \mid x \in A \text{ or } x \in B \text{ but not both. } \} \\ AB &= A \cap B. \end{aligned}$$

For any $A \in R$, we define a function $\chi_A \colon X \to \mathbb{Z}_2$ by

$$\chi_A(x) = \begin{cases} \overline{1} & \text{if } x \in A \\ \overline{0} & \text{if } x \notin A \end{cases}$$

(a) Check that $A + \emptyset = A$ and $A + A = \emptyset$.
(b) Show that $\chi_{A+B}(x) = \chi_A(x) + \chi_B(x)$ and $\chi_{AB}(x) = \chi_A(x)\chi_B(x)$.
(c) Show that if $\chi_A = \chi_B$ then $A = B$.
(d) Prove that the definitions above make R into a commutative ring. (You may wish to use (b) and (c) to help check some of the axioms.)

Solution:

(a) We have $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$ so $A + \emptyset = A \setminus \emptyset = A$. Similarly, we have $A \cup A = A = A \cap A$, so $A + A = A \setminus A = \emptyset$.
(b) For the equation $\chi_{A+B}(x) = \chi_A(x) + \chi_B(x)$, there are four cases to consider.
  (i) x lies in both A and B, so x does not lie in $A + B$, so $\chi_{A+B}(x) = \overline{0}$. Here we have $\chi_A(x) + \chi_B(x) = \overline{1} + \overline{1} = \overline{2} = \overline{0}$ (because we are working in $\mathbb{Z}_2$), so $\chi_{A+B}(x) = \chi_A(x) + \chi_B(x)$ as required.
  (ii) x lies in A but not in B, so $x \in A + B$, so $\chi_{A+B}(x) = \overline{1}$. Here we have $\chi_A(x) + \chi_B(x) = \overline{1} + \overline{0} = \overline{1} = \chi_{A+B}(x)$ as required.
  (iii) x lies in B but not in A; this works the same way as in (ii).
  (iv) x lies in neither A nor B. Here it is clear that $\chi_{A+B}(x) = \overline{0} = \overline{0} + \overline{0} = \chi_A(x) + \chi_B(x)$.
  The argument is similar but easier for the equation $\chi_{AB}(x) = \chi_A(x)\chi_B(x)$.
(c) It is clear that $\{x \in X \mid \chi_A(x) = \overline{1}\} = A$. If $\chi_A = \chi_B$ then $\{x \mid \chi_A(x) = \overline{1}\} = \{x \mid \chi_B(x) = \overline{1}\}$, so $A = B$.
(d) It is clear that the above rules do indeed define subsets of X, so R is closed under addition and multiplication. It is easy to see that $AB = A \cap B = B \cap A = BA$ and $(AB)C = (A \cap B) \cap C = A \cap (B \cap C) = A(BC)$, so multiplication is commutative and associative. Moreover, for $A \subseteq X$ we have $X \cap A = A$, so X is a multiplicative identity element.

  It is also clear that $A + B = B + A$, so addition and is commutative. Part (a) says that $\emptyset$ is an additive identity, and A is an additive inverse for itself. We next show that addition

is associative. By part (b), we have

$$\chi_{A+(B+C)}(x) = \chi_A(x) + \chi_{B+C}(x) = \chi_A(x) + \chi_B(x) + \chi_C(x) = \chi_{A+B}(x) + \chi_C(x) = \chi_{(A+B)+C}(x).$$

It follows using (c) that $A + (B + C) = (A + B) + C$, as required.

All that is left is to check distributivity, which can be done by the same method. We have

$$\begin{aligned}\chi_{A(B+C)}(x) &= \chi_A(x)\chi_{B+C}(x)\\ &= \chi_A(x)(\chi_B(x) + \chi_C(x))\\ &= \chi_A(x)\chi_B(x) + \chi_A(x)\chi_C(x)\\ &= \chi_{AB}(x) + \chi_{AC}(x)\\ &= \chi_{AB+AC}(x),\end{aligned}$$

so $A(B + C) = AB + AC$ as required.

2. Modules

Q6: List all the elements of the Abelian group $\mathbb{Z}_2 \oplus \mathbb{Z}_5$. Find an element that has order 10.

Solution: The elements are $(\overline{0}, \overline{0})$, $(\overline{0}, \overline{1})$, $(\overline{0}, \overline{2})$, $(\overline{0}, \overline{3})$, $(\overline{0}, \overline{4})$, $(\overline{1}, \overline{0})$, $(\overline{1}, \overline{1})$, $(\overline{1}, \overline{2})$, $(\overline{1}, \overline{3})$ and $(\overline{1}, \overline{4})$. I claim that the element $x := (\overline{1}, \overline{1})$ has order 10. Indeed, we have $nx = (\overline{n}, \overline{n})$. The first $\overline{n}$ is in $\mathbb{Z}_2$, so it is zero iff n is divisible by 2. The second $\overline{n}$ is in $\mathbb{Z}_5$, so it is zero iff n is divisible by 5. Thus $nx = (\overline{0}, \overline{0})$ iff n is divisible by both 2 and 5, or equivalently iff n is divisible by 10. This means that x has order 10 as claimed.

Q7:

(a) Calculate $(1 + D + D^2/2 + D^3/6).t^3$. What do you notice? Can you guess a generalisation?
(b) Put $f(t) = e^{-t}\sin(t)$ so $f \in C^\infty(\mathbb{R}, \mathbb{R})$. Calculate $(D + 1)^2 f$.
(c) Put $g_k(t) = t^k e^t$, so $g_k \in C^\infty(\mathbb{R}, \mathbb{R})$. Calculate $(D - 1)g_k$ and thus $(D - 1)^k g_k$. (You may wish to try $k = 3$ first.)
(d) Put $f(t) = te^t$. Show that $(D^k f)(t) = (k + t)e^t$ for all $k \geq 0$ and thus that $(p(D)f)(t) = (p'(1) + p(1)t)e^t$.

Solution:

(a) We have $D.t^3 = 3t^2$ so $D^2.t^3 = 3D.t^2 = 6t$ so $D^3.t^3 = 6D.t = 6$. This means that $(D^2/2).t^3 = 3t$ and $(D^3/6).t^3 = 1$ so $(1 + D + D^2/2 + D^3/6).t^3 = t^3 + 3t^2 + 3t + 1$. We notice that this is just $(t + 1)^3$. The generalisation is that

$$(\sum_{k=0}^{m} D^k/k!).t^m = (t + 1)^m.$$

More generally, if $f(t)$ is any polynomial of degree less than or equal to m, it can be shown that

$$(\sum_{k=0}^{m} D^k/k!).f(t) = f(t + 1).$$

This is essentially Taylor's theorem.

(b) Put

$$g(t) = ((D + 1)f)(t) = f'(t) + f(t) = (-e^{-t}\sin(t) + e^{-t}\cos(t)) + e^{-t}\sin(t) = e^{-t}\cos(t).$$

Then $((D + 1)^2 f)(t) = ((D + 1)g)(t) = g'(t) + g(t) = -e^{-t}\sin(t)$, by a similar calculation. In other words $(D + 1)^2 f = -f$.

(c) We have $((D-1)g_k)(t) = g_k'(t) - g_k(t) = (kt^{k-1}e^t + t^k e^t) - t^k e^t = kt^{k-1}e^t$, or in other words $(D-1)g_k = kg_{k-1}$. It follows that

$$(D-1)^2 g_k = k(D-1)g_{k-1} = k(k-1)g_{k-2}$$
$$(D-1)^3 g_k = k(k-1)(D-1)g_{k-2} = k(k-1)(k-2)g_{k-3}$$

and so on. We eventually find that $(D-1)^k g_k = k! g_0$, so $((D-1)^k g_k)(t) = k!e^t$.

(d) We certainly have $(D^0 f)(t) = f(t) = (0+t)e^t$. Assuming that $(D^k f)(t) = (k+t)e^t$ for some particular value of k, we have

$$(D^{k+1}f)(t) = D((k+t)e^t) = (k+t)D(e^t) + e^t D(k+t) = (k+t)e^t + e^t = ((k+1)+t)e^t.$$

It follows by induction that $(D^k f)(t) = (k+t)e^t$ for all k. Thus, for an operator $p(D) = \sum_k a_k D^k$, we have

$$(p(D)f)(t) = \sum_k a_k(k+t)e^t = ((\sum_k k a_k) + (\sum_k a_k)t)e^t.$$

We also have $p(1) = \sum_k a_k . 1^k = \sum_k a_k$. Similarly, we have $p'(D) = \sum_k k a_k D^{k-1}$, so $p'(1) = \sum_k k a_k$. Putting these into our earlier formula gives

$$(p(D)f)(t) = (p'(1) + p(1)t)e^t,$$

as claimed.

Q8: Define $v(t) = e^{t^2/2}$, so $u \in C^\infty(\mathbb{R}, \mathbb{R})$. Let V be the set of functions of the form $f(t)v(t)$, where f is a polynomial. For example, the function $(1 + t + t^2)e^{t^2/2}$ is an element of V.

(a) Prove that V is an $\mathbb{R}[D]$-submodule of $C^\infty(\mathbb{R}, \mathbb{R})$.
(b) Calculate $D^k v$ for $0 \leq k \leq 3$.
(c) Show that for all $k \geq 0$ there is a polynomial $p_k(t)$ of the form $t^k +$ lower terms such that $D^k v = p_k . v$.
(d) Show that if $q(D)$ is a nonzero element of $\mathbb{R}[D]$ then $q(D)v \neq 0$ (look at leading terms).
(e) Suppose that $f(t)$ is a polynomial of degree k, say $f(t) = at^k +$ lower terms . Prove by induction on k that $fv = q(D)v$ for some element $q(D) \in \mathbb{R}[D]$.
(f) Deduce that $V \simeq \mathbb{R}[D]$ as an $\mathbb{R}[D]$-module.

Solution:

(a) We just need to check that V is closed under differentiation. Note that $v'(t) = te^{t^2/2} = tv(t)$, so

$$\frac{d}{dt} f(t)v(t) = f(t)v'(t) + f'(t)v(t) = (tf(t) + f'(t))v(t).$$

If $f(t)$ is a polynomial, then clearly $tf(t) + f'(t)$ is also a polynomial, so the function $(tf(t) + f'(t))v(t)$ lies in V as required.

(b) If we differentiate repeatedly using the above rule we find that

$$(D^0 v)(t) = v(t)$$
$$(D^1 v)(t) = tv(t)$$
$$(D^2 v)(t) = (t^2+1)v(t)$$
$$(D^3 v)(t) = (t^3 + 3t)v(t).$$

(c) As V is an $\mathbb{R}[D]$-module, we must have $D^k v \in V$, so $D^k v = p_k v$ for some polynomial p_k. (From part (b) we see that $p_0(t) = 1$, $p_1(t) = t$, $p_2(t) = t^2 + 1$ and $p_3(t) = t^3 + 3t$.) Using part (a) we see that $p_{k+1}(t) = tp_k(t) + p_k'(t)$. The claim is that $p_k(t) = t^k +$ lower terms . If this is true for some value of k, then $tp_k(t) = t^{k+1} +$ lower terms and $p_k'(t) = kt^{k-1} +$ lower terms , so $p_{k+1}(t) = t^{k+1} +$ lower terms , so the claim holds for the next value of k. Moreover, the claim visibly holds for $k = 0$, so it holds for all k by induction.

(d) Let k be the degree of q, so $q(D) = a_0 + a_1 D + \ldots + a_k D^k$ for some $a_0, \ldots, a_k \in \mathbb{R}$ with $a_k \neq 0$. Then $q(D)v = (a_0 p_0 + \ldots + a_k p_k)v$, and using part (c) we see that $a_0 p_0(t) + \ldots + a_k p_k(t) = a_k t^k +$ lower terms , so in particular it is not zero.

(e) First suppose that f has degree 0, say $f(t) = c$ for all t, where $c \in \mathbb{R}$. We can regard c as an element in $\mathbb{R}[D]$, and $fv = cv$ as required; this proves the claim for $k = 0$.

Now suppose we have proved the claim for all polynomials of degree less than k, and that f has degree k. Then $f(t) = at^k +$ lower terms for some $a \in \mathbb{R}$. It follows that the function $g(t) = f(t) - ap_k(t)$ is a polynomial of degree less than k, so we have $gv = q(D)v$ for some $q(D) \in \mathbb{R}[D]$. It follows that

$$fv = gv + ap_k v = q(D)v + aD^k v = (q(D) + aD^k)v,$$

so $fv \in \mathbb{R}[D]v$ as required. The claim now follows for all degrees by induction.

(f) We know from part (e) that v generates V as an $\mathbb{R}[D]$-module. It follows that $V \simeq \mathbb{R}[D]/I$, where $I = \{q(D) \in \mathbb{R}[D] \mid q(D)v = 0\}$. Part (d) tells us that $I = 0$, so $V \simeq \mathbb{R}[D]$.

3. Modules over polynomial rings

Q9: Let A be the matrix $\begin{pmatrix} 1&1&0&0 \\ 0&1&1&0 \\ 0&0&1&1 \\ 0&0&0&1 \end{pmatrix}$. Find A^2, A^3 and A^4. Can you give a general rule for A^n?

Solution: The first few powers are

$$A^2 = \begin{pmatrix} 1&2&1&0 \\ 0&1&2&1 \\ 0&0&1&2 \\ 0&0&0&1 \end{pmatrix}$$

$$A^3 = \begin{pmatrix} 1&3&3&1 \\ 0&1&3&3 \\ 0&0&1&3 \\ 0&0&0&1 \end{pmatrix}$$

$$A^4 = \begin{pmatrix} 1&4&6&4 \\ 0&1&4&6 \\ 0&0&1&4 \\ 0&0&0&1 \end{pmatrix}$$

In general, in the matrix A^n all the entries in the k'th band above and parallel to the diagonal are equal to the binomial coefficient $\binom{n}{k}$. The entries below the diagonal are zero.

Q10:

(a) Put $A = \begin{pmatrix} 1&0&1 \\ 0&1&0 \\ 0&0&1 \end{pmatrix}$ and $m = (1,1,1) \in M_A$. Calculate $(x^3 - 1)m$.

(b) Put $A = \begin{pmatrix} 0&0&1 \\ 0&1&0 \\ 1&0&0 \end{pmatrix}$ and $m = (1,2,3) \in M_A$. Calculate $(x^3 - 1)m$.

(c) Put $A = \begin{pmatrix} 1&1 \\ 1&1 \end{pmatrix}$ and $m = (1,-1) \in M_A$. Calculate $(14x^{12} + 5x^{11} - 36x^7 - 22x^4 + 13x - 5)m$. (You may wish to start by calculating fm for some very simple polynomials f first.)

Solution:

(a) $A^3 - I = \begin{pmatrix} 0&0&3 \\ 0&0&0 \\ 0&0&0 \end{pmatrix}$ so

$$(x^3 - 1)m = \begin{pmatrix} 0&0&3 \\ 0&0&0 \\ 0&0&0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \\ 0 \end{pmatrix}.$$

(b) $A^2 = I$ so $A^3 = A$ so $A^3 - I = A - I$. Moreover $Am = (3,2,1)$ so $(A - I)m = Am - m = (3,2,1) - (1,2,3) = (2,0,-2)$. Thus $(x^3 - 1)m = (2,0,-2)$.

(c) $Am = (0,0)$ so $x^k m = A^k m = 0$ for all $k > 0$. Thus when we expand out $(14x^{12} + 5x^{11} - 36x^7 - 22x^4 + 13x - 5)m$, all the terms except the last one are zero, so we are left with $-5m = (-5,5)$.

Q11: Let $A = \begin{pmatrix} a&b \\ c&d \end{pmatrix}$ be a 2×2 matrix, and put $f(x) = x^2 - (a+d)x + (ad - bc)$. Show that $f(A) = \begin{pmatrix} 0&0 \\ 0&0 \end{pmatrix}$. (This is the 2×2 case of the Cayley-Hamilton theorem.)

Solution: We have

$$A^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{pmatrix}$$

and

$$(a+d)A = \begin{pmatrix} a^2+ad & ab+bd \\ ac+cd & ad+d^2 \end{pmatrix}$$

so

$$\begin{aligned} f(A) &= A^2 - (a+d)A + (ad-bc)I \\ &= \begin{pmatrix} a^2+bc & ab+bd \\ ac+cd & bc+d^2 \end{pmatrix} - \begin{pmatrix} a^2+ad & ab+bd \\ ac+cd & ad+d^2 \end{pmatrix} + \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

Q12: Put $A = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ and $f(x) = x^4 - 3x$. Calculate $f(A)$.

Solution: $A^2 = \left(\begin{smallmatrix} 2 & 2 \\ 2 & 2 \end{smallmatrix}\right) = 2A$ so $A^4 = (A^2)^2 = (2A)^2 = 4A^2 = 8A$. Thus $f(A) = A^4 - 3A = 8A - 3A = 5A = \left(\begin{smallmatrix} 5 & 5 \\ 5 & 5 \end{smallmatrix}\right)$.

Q13: Consider the matrix

$$A = \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right),$$

and a polynomial $f(x) = \sum_i a_i x^i$.

(a) Calculate A^i for some small numbers i, then give the general rule.
(b) Write $b = a_0 + a_2 + a_4 + \ldots = \sum_j a_{2j}$ and $c = a_1 + a_3 + \ldots = \sum_j a_{2j+1}$. Express $f(1)$ and $f(-1)$ in terms of b and c.
(c) Show that

$$f(A) = \frac{f(1)}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \frac{f(-1)}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}.$$

Solution:

(a) Clearly $A^0 = I$ and $A^1 = A$. We observe that $A^2 = I$, and it follows immediately that A^i is I whenever i is even, and A whenever i is odd.
(b) We have $f(1) = \sum_i a_i = b + c$, and $f(-1) = \sum_i (-1)^i a_i = b - c$. It follows that $b = (f(1) + f(-1))/2$ and $c = (f(1) - f(-1))/2$.
(c) We have $f(A) = \sum_i a_i A^i$. The term corresponding to an even number $i = 2j$ is $a_{2j} I$, whereas the term corresponding to an odd number $i = 2j+1$ is $a_{2j+1} A$. We thus have

$$\begin{aligned} f(A) &= \sum_j (a_{2j} I + a_{2j+1} A) \\ &= bI + cA \\ &= ((f(1) + f(-1))/2)I + ((f(1) - f(-1))/2)A \\ &= f(1)(I+A)/2 + f(-1)(I-A)/2 \\ &= \frac{f(1)}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \frac{f(-1)}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}. \end{aligned}$$

4. General module theory

Q14: Let $\alpha\colon M \to N$ be a homomorphism of modules over $\mathbb{C}[x]$. Suppose that $(x^3 - x)M = \{0\}$ and $x^5 N = \{0\}$. Prove that for $n \in \text{image}(\alpha)$ we have $xn = 0$. Can you formulate a general theorem of which this is a special case?

Solution: Let $\alpha\colon M \to N$ be a homomorphism of modules over a Euclidean domain R. Suppose that $aM = \{0\}$ and $bN = \{0\}$ and let c be the gcd of a and b. I claim that $cn = 0$ for all $n \in \text{image}(\alpha)$. Indeed, we can write $c = au + bv$ for some $a, b \in R$. If $n \in \text{image}(\alpha)$ then $n = \alpha(m)$ for some $m \in M$. We have $am = 0$ (because $aM = \{0\}$) so $an = a\alpha(m) = \alpha(am) = \alpha(0) = 0$. We also have $n \in N$ and $bN = \{0\}$ so $bn = 0$. Thus $cn = uan + vbn = 0 + 0 = 0$ as claimed.

In the case considered we have $R = \mathbb{C}[x]$ and $a = x^3 - x = (x-1)(x+1)x$ and $b = x^5$ so it is clear that $c = x$. Thus $xn = 0$ for all $n \in \text{image}(\alpha)$.

Q15: Let R be a ring, and let M and N be R-modules. Show that if $M \oplus N$ is cyclic, then so are M and N.

Solution: Suppose that $M \oplus N$ is cyclic, so there is an element $(x, y) \in M \oplus N$ as an R-module. This means that for any element $(m, n) \in M \oplus N$, there exists $a \in R$ such that $a(x, y) = (m, n)$. In particular, for any element $m \in M$ we have $(m, 0) \in M \oplus N$, so there exists $a \in R$ such that $a(x, y) = (m, 0)$, which means that $m = ax$. This shows that M is generated by the single element x, so M is cyclic. Similarly, N is generated by y and so is cyclic.

Q16:

(a) Put $N_0 = \{(n, m) \in \mathbb{Z}^2 \mid n - m \text{ is even }\}$ and $N_1 = \{(n, m) \in \mathbb{Z}^2 \mid n - m \text{ is odd }\}$. Are these $\mathbb{Z}$-submodules of $\mathbb{Z}^2$?

(b) Put $A = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ and $N_0 = \{(u, v) \in \mathbb{R}^2 \mid u - v = 0\}$ and $N_1 = \{(u, v) \mid u + v = 0\}$. Are these $\mathbb{R}[x]$-submodules of M_A?

(c) Put $N_0 = \{f \in C^\infty(\mathbb{R}, \mathbb{R}) \mid f(1) = 0\}$ and $N_1 = \{f \in C^\infty(\mathbb{R}, \mathbb{R}) \mid \int_0^2 f = 0\}$. Are these $\mathbb{R}[D]$-submodules of $C^\infty(\mathbb{R}, \mathbb{R})$?

Solution:

(a) The set N_1 is not a submodule, because $(1, 0) \in N_1$ but $2(1, 0) = (2, 0) \notin N_1$. However, the set N_0 is a submodule. To see this, suppose that (n, m) and (n', m') lie in N_0, so $n - m$ and $n' - m'$ are even. Then $(n, m) + (n', m') = (n + n', m + m')$ and the integer $(n + n') - (m + m') = (n - m) + (n' - m')$ is even so $(n, m) + (n', m') \in N_0$. Similarly, for any $a \in \mathbb{Z}$ we have $a(n, m) = (an, am)$ and $an - am = a(n - m)$ is even, so $a(n, m) \in N_0$. It is clear that $(0, 0) \in N_0$ and it follows that N_0 is a submodule as claimed.

(b) I claim that both N_0 and N_1 are submodules of M_A. It is clear that they are both vector subspaces of $\mathbb{R}^2$, so it is enough to check that they are both stable under A. An element $w \in N_0$ has the form $w = \left(\begin{smallmatrix} x \\ x \end{smallmatrix}\right)$ so $Aw = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} x \\ x \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2x \\ 2x \end{smallmatrix}\right)$, so $Aw \in N_0$. This shows that N_0 is stable under A and thus is a submodule. Similarly, an element $w \in N_1$ has the form $w = \left(\begin{smallmatrix} x \\ -x \end{smallmatrix}\right)$ so $Aw = \left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right)$. As the zero vector certainly lies in N_1 we have $Aw \in N_1$ and so N_1 is also stable under A.

(c) I claim that neither N_0 nor N_1 is an $\mathbb{R}[D]$-submodule of $C^\infty(\mathbb{R}, \mathbb{R})$. Indeed, put $f(t) = t - 1$, so $f \in C^\infty(\mathbb{R}, \mathbb{R})$. Then $f(0) = 0$, so $f \in N_0$. However, $f'(0) = 1 \neq 0$, so $f' \notin N_0$, so N_0 is not closed under differentiation, so it is not an $\mathbb{R}[D]$-submodule of $C^\infty(\mathbb{R}, \mathbb{R})$. To prove that N_1 is not a submodule, we can use the same function f. We have $\int_0^2 f = [t^2/2 - t]_0^2 = 0$, so $f \in N_1$. However, $\int_0^2 f' = \int_0^2 1 = 2$, so $f' \notin N_1$, so N_1 is not a submodule.

Q17: Let R be a ring with exactly 10 elements, and let M be an R-module with exactly 20 elements. Prove that M is not a free module.

Solution: If M were free, it would be isomorphic to R^d for some d, so we would have $20 = |M| = |R^d| = |R|^d = 10^d$. As 20 is not a power of 10, this is impossible, so M cannot be free.

Q18: For any integer d, let N_d be the submodule of $\mathbb{Z}_{24}$ generated by $\overline{d}$. The group N_6 has precisely 4 elements; list them. Find integers d and e such that $N_6 \cap N_4 = N_d$ and $N_6 + N_4 = N_e$.

Solution: The elements of N_6 are the multiples of $\overline{6}$, which are $\overline{0}$, $\overline{6}$, $\overline{12}$ and $\overline{18}$. We can stop at this point because $\overline{24} = \overline{0}$, $\overline{30} = \overline{6}$ and so on. Thus $N_6 = \{\overline{0}, \overline{6}, \overline{12}, \overline{18}\}$, and similarly we have $N_4 = \{\overline{0}, \overline{4}, \overline{8}, \overline{12}, \overline{16}, \overline{20}\}$. From this we see that $N_4 \cap N_6 = \{\overline{0}, \overline{12}\} = N_{12}$, so we can take $d = 12$.

As $\overline{8} \in N_4$ and $\overline{18} \in N_6$, the group $N_4 + N_6$ contains $\overline{8} + \overline{18} = \overline{26} = \overline{2}$. As $N_4 + N_6$ is a subgroup of $\mathbb{Z}_{24}$ we deduce that all multiples of $\overline{2}$ lie in $N_4 + N_6$, so $N_2 \subseteq N_4 + N_6$. On the other hand, as 4, 6 and 24 are all even we see that all elements of $N_4 + N_6$ have the form $\overline{a}$ for some even integer a and thus they lie in N_2. This shows that $N_4 + N_6 = N_2$, so we can take $e = 2$.

Q19: For any natural number d dividing 900, let N_d be the submodule of $\mathbb{Z}_{900}$ generated by $\overline{d}$.

(a) What is the order of N_{10}?
(b) Which standard group is isomorphic to $\mathbb{Z}_{900}/N_{10}$?
(c) Find d such that the submodule generated by $\overline{70}$ is N_d.
(d) Find d such that $N_{12} + N_{30} + N_{100} = N_d$.
(e) Find d such that $N_{30} \cap N_{50} = N_d$.

Solution:

(a) The order is $900/10 = 90$.
(b) The factor group $\mathbb{Z}_{900}/N_{10}$ is isomorphic to $\mathbb{Z}_{10}$.
(c) Here d is the greatest common divisor of 70 and 900, which is 10.
(d) Here d is the greatest common divisor of $12 = 2^2 \times 3$, $30 = 2 \times 3 \times 5$ and $100 = 2^2 \times 5^2$, so $d = 2$.
(e) Here d is the least common multiple of $30 = 2 \times 3 \times 5$ and $50 = 2 \times 5^2$, so $d = 2 \times 3 \times 5^2 = 150$.

Q20: Consider the following matrix over $\mathbb{Q}$.

$$A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Show that the module M_A over $\mathbb{Q}[x]$ is cyclic, and give a polynomial $f(x)$ such that $M_A \simeq \mathbb{Q}[x]/f(x)$.

Solution: Put $u = (1, 0, 0)$. Then $xu = (0, 0, 1)$ and $x^2u = (1, 1, 1)$. These three vectors are clearly linear independent, so they form a basis of $\mathbb{Q}^3$, so they span $\mathbb{Q}^3$. Thus any vector $v \in \mathbb{Q}^3$ can be written in the form $au + bxu + cx^2u$ for some $a, b, c \in \mathbb{Q}$. In other words, $v = (a + bx + cx^2)u \in \mathbb{Q}[x]u$, so we see that u generates M_A as a $\mathbb{Q}[x]$-module. This means that $M_A \simeq \mathbb{Q}[x]/f(x)$ for some polynomial $f(x)$, which we can assume is monic. From the general theory we know that the degree of f is the size of A, which is 3. We also know that $f(x)$ is the only monic polynomial of degree 3 such that $f(x).u = 0$.

The polynomial f is in fact the characteristic polynomial of A, which can be calculated directly:

$$\det(xI - A) = \begin{vmatrix} x & 0 & -1 \\ 0 & x-1 & -1 \\ -1 & -1 & x-1 \end{vmatrix} = x^3 - 2x^2 - x + 1.$$

For another approach, consider the vector $x^3u = x(1,1,1) = (1,2,3)$. We would like to write this in the form $au + bxu + cx^2u$, so we want

$$(1,2,3) = a(1,0,0) + b(0,0,1) + c(1,1,1) = (a+c, c, b+c).$$

The solution is $a = -1, b = 1, c = 2$, so $x^3u = -u + xu + 2x^2u$, so $(x^3 - 2x^2 - x + 1)u = 0$, so $f(x) = x^3 - 2x^2 - x + 1$.

Q21: Let W_d be the set of polynomials $f(t)$ of degree at most d. Prove that W_d is a cyclic module over $\mathbb{R}[D]$. What is the ideal $I \subseteq \mathbb{R}[D]$ such that $W_d \simeq \mathbb{R}[D]/I$?

Solution: Define $\alpha\colon \mathbb{R}[D] \to W_d$ by $\alpha(p(D)) = p(D).t^d$. Note that

$$\begin{aligned} D.t^d &= dt^{d-1} \\ D^2.t^d &= d(d-1)t^{d-2} \\ D^3.t^d &= d(d-1)(d-2)t^{d-3} \end{aligned}$$

and so on. In general, we have $D^k.t^d = m_k t^{d-k}$, where $m_k = d(d-1)\dots(d-k+1) = \prod_{i=0}^{k-1}(d-i)$, as one can easily check by induction. Note also that when $k \leq d$ all the factors $d-i$ for $0 \leq i \leq k-1$ are nonzero, so $m_k \neq 0$. However, we have $m_k = 0$ for $k > d$. Any element $f(t) \in W_d$ has the form $f(t) = a_0 + a_1 t + \dots + a_d t^d$ for some $a_0, \dots, a_d \in \mathbb{R}$. If we define

$$p(D) = \sum_{i=0}^{d} a_{d-i} D^i / m_i = a_d + a_{d-1} D/m_1 + \dots + a_0 D^d/m_d$$

we find that

$$\begin{aligned} p(D).t^d &= a_d t^d + a_{d-1} m_1^{-1} D.t^d + \dots + a_0 m_d^{-1} D^d.t^d \\ &= a_d t^d + a_{d-1} t^{d-1} + \dots + a_0 t^0 \\ &= f(t). \end{aligned}$$

Thus every element $f \in W_d$ has the form $f = p(D).t^d$ for some $p(D) \in \mathbb{R}[D]$, so W_d is generated by t^d as a module over $\mathbb{R}[D]$.

Now put $I = \{p \in \mathbb{R}[D] \mid p(D).t^d = 0\}$, so $W_d \simeq \mathbb{R}[D]/I$. Suppose we have an element $p(D) = \sum_i b_i D^i \in \mathbb{R}[D]$. Then $p(D).t^d = b_0 t^d + b_1 m_1 t^{d-1} + \dots + b_d m_d t^0$, and this is zero iff $b_0 = \dots = b_d = 0$. This means that $p(D)$ has the form $b_{d+1}D^{d+1} + b_{d+2}D^{d+2} + \dots$, so it is divisible by D^{d+1}. Thus I is the principal ideal $\mathbb{R}[D].D^{d+1}$, and $W_d \simeq \mathbb{R}[D]/D^{d+1}$.

Q22: Fix a nonzero vector $u \in \mathbb{R}^3$, and write $r = \|u\|$. Define an endomorphism $\phi\colon \mathbb{R}^3 \to \mathbb{R}^3$ by $\phi(v) = u \times v$. Write M for $\mathbb{R}^3$, considered as a module over $\mathbb{R}[x]$ using ϕ. Let L be the line through u and 0, and let K be the plane perpendicular to L.

(a) Show that L is a submodule of M, and that $xL = 0$.
(b) Show that K is a submodule of M, and that $(x^2 + r^2)K = 0$ and $xM \leq K$.
(c) Show that $(x^3 + r^2 x)M = 0$.

(You will need a number of standard facts about dot and cross products of vectors.)

Solution:

(a) If $v \in L$ then $v = tu$ for some $t \in \mathbb{R}$, so $xv = \phi(v) = t(u \times u) = 0$ (using the fact that $a \times a = 0$ for any vector a). This shows that $xL = \phi(L) = 0$, so certainly $\phi(L) \leq L$, so L is a submodule.

(b) For any $v \in M$ we have $xv = \phi(v) = u \times v$, which is always perpendicular to u, so it lies in K. This says that $xM = \phi(M) \leq K$, so certainly $\phi(K) \leq K$, so K is a submodule. Next, for any $v \in K$ we have $u.v = 0$ and so

$$x^2 v = \phi^2(v) = u \times (u \times v) = (u.v)u - (u.u)v = 0u - r^2 v = -r^2 v,$$

so $(x^2 + r^2)v = 0$. This shows that $(x^2 + r^2)K = 0$ as claimed.

(c) We now know that $xM \leq K$ so

$$(x^3 + r^2x)M = (x^2 + r^2)xM \leq (x^2 + r^2)K = 0.$$

5. Homomorphisms

Q23: In each of the following situations, find all the $\mathbb{Q}[x]$-module homomorphisms from M_A to M_B.

(a) $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.
(b) $A = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} \mu & 0 \\ 0 & \lambda \end{smallmatrix}\right)$, where $\lambda \neq \mu$.
(c) $A = I_2$ (the 2×2 identity matrix) and $B = I_3$.

Solution: Such homomorphisms correspond to matrices P of the appropriate shape (the same number of columns as A, and the same number of rows as B) such that $PA = BP$.

(a) Here P is a 2×2 matrix, say $P = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. We have $PA = \left(\begin{smallmatrix} a & a+b \\ c & c+d \end{smallmatrix}\right)$ and $BP = \left(\begin{smallmatrix} c & d \\ a & b \end{smallmatrix}\right)$. Thus $PA = BP$ if and only if $a = c$, $a + b = d$, $c = a$ and $c + d = b$. By solving these equations we find that $c = a = 0$ and $d = b$. Thus, the homomorphisms from M_A to M_B are precisely the matrices of the form $P = \left(\begin{smallmatrix} 0 & b \\ 0 & b \end{smallmatrix}\right)$ over $\mathbb{Q}$.
(b) Here again we have $P = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ for some a, b, c, d. Thus $PA = \left(\begin{smallmatrix} \lambda a & \mu b \\ \lambda c & \mu d \end{smallmatrix}\right)$ and $BP = \left(\begin{smallmatrix} \mu a & \mu b \\ \lambda c & \lambda d \end{smallmatrix}\right)$, so $PA = BP$ if and only if $\lambda a = \mu a$ and $\mu d = \lambda d$, or in other words $(\lambda - \mu)a = (\lambda - \mu)d = 0$. As $\lambda - \mu \neq 0$ this means that $a = d = 0$. Thus, the homomorphisms from M_A to M_B are precisely the matrices of the form $P = \left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right)$.
(c) Here P is a 2×3 matrix over $\mathbb{Q}$. We have $PA = PI_2 = P$ and $BP = I_3P = P$ so the condition $PA = BP$ is automatically satisfied. Thus the homomorphisms from M_A to M_B are all the 2×3 matrices over $\mathbb{Q}$.

Q24:

(a) Put $A = \left(\begin{smallmatrix} 1 & 2 \\ 0 & 2 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$. Find all the $\mathbb{Q}[x]$-module homomorphisms from M_A to M_B.
(b) Put $A = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$. Find all the $\mathbb{Q}[x]$-module homomorphisms from M_A to M_B.
(c) Suppose that $\lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2 \in \mathbb{C}$, and put $A = \left(\begin{smallmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} \mu_1 & 0 \\ 0 & \mu_2 \end{smallmatrix}\right)$. Show that for most values of the λ's and μ's, the only $\mathbb{C}[x]$-module homomorphism from M_A to M_B is zero. What can you say about the exceptional cases?

Solution:

(a) The homomorphisms correspond to matrices $C = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $CA = BC$, or equivalently $\left(\begin{smallmatrix} a & 2a+2b \\ c & 2c+2d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a+c & b+d \\ a+c & b+d \end{smallmatrix}\right)$, so

$$\begin{aligned} a &= a + c \\ 2a + 2b &= b + d \\ c &= a + c \\ 2c + 2d &= b + d. \end{aligned}$$

The first and third equations give $a = c = 0$, and the remaining equations then give $d = b$, so C must have the form $\left(\begin{smallmatrix} 0 & b \\ 0 & b \end{smallmatrix}\right)$.
(b) We need to find the 3×3 matrices with $CA = BC$. Note that $BC = C$. Put $D = A - I = \left(\begin{smallmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{smallmatrix}\right)$. The condition $CA = BC$ now becomes $C(I + D) = C$, or equivalently $CD = 0$. If the columns of C are u, v and w, then the columns of CD are easily seen to be v, w and 0. Thus $CD = 0$ iff $v = w = 0$, so all the nonzero entries of C must be in the first column. Thus the homomorphisms from M_A to M_B are the matrices of the form $\left(\begin{smallmatrix} a & 0 & 0 \\ b & 0 & 0 \\ c & 0 & 0 \end{smallmatrix}\right)$.

(c) Here we need the matrices $C = \begin{pmatrix} c_{11} & c_{21} & c_{31} \\ c_{12} & c_{22} & c_{32} \end{pmatrix}$ such that

$$\begin{pmatrix} c_{11} & c_{21} & c_{31} \\ c_{12} & c_{22} & c_{32} \end{pmatrix} \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix} = \begin{pmatrix} \mu_1 & 0 \\ 0 & \mu_2 \end{pmatrix} \begin{pmatrix} c_{11} & c_{21} & c_{31} \\ c_{12} & c_{22} & c_{32} \end{pmatrix},$$

or equivalently

$$\begin{pmatrix} (\lambda_1 - \mu_1)c_{11} & (\lambda_2 - \mu_1)c_{21} & (\lambda_3 - \mu_1)c_{31} \\ (\lambda_1 - \mu_2)c_{11} & (\lambda_2 - \mu_2)c_{21} & (\lambda_3 - \mu_2)c_{31} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

For most choices of numbers $\lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2$, the λ's will all be different from the μ's, so all the numbers $\lambda_i - \mu_j$ will be nonzero. In this case, the only possible matrix C is the zero matrix. In general, if we have $\lambda_i = \mu_j$ for some pairs (i, j), then the corresponding entries c_{ij} can be nonzero.

Q25: Let a be an element of a ring R. For any R-module M, put

$$\operatorname{ann}(a, M) = \{m \in M \mid am = 0\}.$$

We will also write R/a for the factor module R/Ra.

(a) Find $\operatorname{ann}(4, \mathbb{Z}_{12})$.
(b) Find $\operatorname{ann}(x - 1, M_A)$, where A is the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$.
(c) Let $\alpha\colon R/a \to M$ be a homomorphism. Show that $\alpha(\overline{1}) \in \operatorname{ann}(a, M)$.
(d) Conversely, given $m \in \operatorname{ann}(a, M)$, show that there is a unique homomorphism $\alpha\colon R/a \to M$ such that $\alpha(\overline{1}) = m$.
(e) Describe all the $\mathbb{R}[D]$-module homomorphisms from $\mathbb{R}[D]/(D^2 - 1)$ to $C^\infty(\mathbb{R}, \mathbb{R})$.

Solution:

(a) $\operatorname{ann}(4, \mathbb{Z}_{12}) = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} \simeq \mathbb{Z}_4$.
(b) We have

$$(x - 1)(u, v) = (A - I)(u, v) = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} 0 \\ u \end{pmatrix},$$

so $(x - 1)(u, v) = (0, 0)$ iff $u = 0$. Thus $\operatorname{ann}(x - 1, M_A) = \{(0, v) \mid v \in \mathbb{R}\}$.
(c) $a\alpha(\overline{1}) = \alpha(a.\overline{1}) = \alpha(\overline{a}) = \alpha(\overline{0}) = 0$, because $\overline{a} = \overline{0}$ in R/a.
(d) Suppose that $m \in \operatorname{ann}(a, M)$. We can certainly define a homomorphism $\beta\colon R \to M$ by $\beta(x) = xm$. As $am = 0$ this satisfies $\beta(ya) = yam = 0$, so $\beta(x) = 0$ for $x \in Ra$. By the first isomorphism theorem we get an induced map $\alpha = \overline{\beta}\colon R/aR \to M$ defined by $\alpha(\overline{x}) = \beta(x) = xm$, and in particular $\alpha(\overline{1}) = m$.
(e) Note that $\operatorname{ann}(D^2 - 1, C^\infty(\mathbb{R}, \mathbb{R}))$ is the space of solutions of the differential equation $f'' = f$, or equivalently the space of functions of the form $f(t) = ue^t + ve^{-t}$ with $u, v \in \mathbb{R}$. For each such function we get a homomorphism $\alpha\colon \mathbb{R}[D]/(D^2 - 1) \to C^\infty(\mathbb{R}, \mathbb{R})$ given by

$$\alpha(\overline{a + bD}) = (a + bD)(ue^t + ve^{-t}) = (a + b)ue^t + (a - b)ve^{-t}.$$

Q26: Show that there are homomorphisms $\alpha\colon \mathbb{Z}_3 \to \mathbb{Z}_9$ and $\beta\colon \mathbb{Z}_9 \to \mathbb{Z}_3$ given by $\alpha(\overline{n}) = \overline{3n}$ and $\beta(\overline{m}) = \overline{m}$. Show that the sequence $\mathbb{Z}_3 \xrightarrow{\alpha} \mathbb{Z}_9 \xrightarrow{\beta} \mathbb{Z}_3$ is exact.

Solution: Recall that there is a map $\phi\colon \mathbb{Z}_p \to \mathbb{Z}_q$ with $\phi(\overline{m}) = \overline{rm}$ iff rp is divisible by q. This is satisfied when $r = p = 3$ and $q = 9$, so α exists. It is also satisfied when $p = 9$ and $r = 1$ and $q = 3$, so β exists.

The elements of $\mathbb{Z}_3$ are $\overline{0}$, $\overline{1}$ and $\overline{2}$. We have $\alpha(\overline{0}) = \overline{0}$, $\alpha(\overline{1}) = \overline{3}$ $\alpha(\overline{2}) = \overline{6}$, so the image of α is $\{\overline{0}, \overline{3}, \overline{6}\}$.

Next, the elements of $\mathbb{Z}_9$ are $\overline{0}, \dots, \overline{8}$. We have $\beta(\overline{3}) = \overline{3}$. The $\overline{3}$ on the left hand side is interpreted as an element of $\mathbb{Z}_9$ and thus is nonzero, but the $\overline{3}$ on the right hand side is interpreted as an element of $\mathbb{Z}_3$ and thus is zero. In other words, we have $\beta(\overline{3}) = \overline{0}$. Similarly, we have

$$\beta(\overline{0}) = \beta(\overline{3}) = \beta(\overline{6}) = \overline{0}$$
$$\beta(\overline{1}) = \beta(\overline{4}) = \beta(\overline{7}) = \overline{1}$$
$$\beta(\overline{2}) = \beta(\overline{5}) = \beta(\overline{8}) = \overline{2}.$$

Thus $\ker(\beta) = \{a \in \mathbb{Z}_9 \mid \beta(a) = \overline{0}\} = \{\overline{0}, \overline{3}, \overline{6}\}$. We have shown that $\ker(\beta) = \text{image}(\alpha)$, so the sequence $\mathbb{Z}_3 \xrightarrow{\alpha} \mathbb{Z}_9 \xrightarrow{\beta} \mathbb{Z}_3$ is exact.

Q27:

(a) Let α be a $\mathbb{C}[x]$-module homomorphism from $\mathbb{C}[x]/(x^2 - 1)$ to M_A, where $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$. Prove that $\alpha = 0$.

(b) Let V be the space of functions of the form $a\sin(t) + b\cos(t)$, and let W be the space of functions of the form $a\sinh(t) + b\cosh(t)$. Let $\beta\colon V \to W$ be an $\mathbb{R}[D]$-module homomorphism. Show that $\beta = 0$.

(c) Let $\gamma\colon \mathbb{Z}_4 \to \mathbb{Z}^4$ be a homomorphism of $\mathbb{Z}$-modules. Prove that $\gamma = 0$.

Solution:

(a) It is easy to see that $A^2 = 3A$, so for all $v \in M_A$ we have $(x^2 - 3x)v = 0$. In particular, for $u \in \mathbb{C}[x]/(x^2 - 1)$ we have $(x^2 - 3x)\alpha(u) = 0$. However, we also have $(x^2 - 1)u = 0$ and so $(x^2 - 1)\alpha(u) = 0$. The polynomials $x^2 - 3x = x(x - 3)$ and $x^2 - 1 = (x - 1)(x + 1)$ are coprime, so there exist polynomials $p(x)$ and $q(x)$ with $p(x)(x^2 - 3x) + q(x)(x^2 - 1) = 1$. It follows that

$$\alpha(u) = p(x)(x^2 - 3x)\alpha(u) + q(x)(x^2 - 1)\alpha(x) = 0 + 0 = 0.$$

As this holds for all $u \in \mathbb{C}[x]/(x^2 - 1)$, we have $\alpha = 0$ as claimed.

(b) As $\sin'' = -\sin$ and $\cos'' = -\cos$ we have $(D^2 + 1)V = 0$. As $\sinh'' = \sinh$ and $\cosh'' = \cosh$ we have $(D^2 - 1)W = 0$. The elements $D^2 + 1$ and $D^2 - 1$ are coprime in $\mathbb{R}[D]$, so $\beta = 0$ by the same argument as in part (a).

(c) We have $\gamma(\overline{1}) = (w, x, y, z) \in \mathbb{Z}^4$ for some $w, x, w, z \in \mathbb{Z}$. As $4.\overline{1} = \overline{0}$ we see that $(4w, 4x, 4y, 4z) = \gamma(\overline{0}) = (0, 0, 0, 0)$, so $4w = 4x = 4y = 4z = 0$. As w, x, y and z are just integers, this implies that $w = x = y = z = 0$, so $\gamma(\overline{1}) = 0$. This in turn implies that $\gamma(\overline{n}) = n.\gamma(\overline{1}) = n.0 = 0$ for all n.

Q28: Let R be a ring, and let M be an R-module with only finitely many elements, say $|M| = m$. How many homomorphisms are there from R^d to M?

Solution: A homomorphism from R^d to M corresponds to a list $(m_1, \dots, m_d)$ of elements of M. There are m possible choices for each entry in the list, so there are m^d possible lists, and thus m^d different homomorphisms from R^d to M.

6. Factor modules

Q29: Let M be a module over a ring R, and let L and N be submodules of M. Prove that $L/(L \cap N)$ is isomorphic to $(L + N)/N$. [You may wish to consider the homomorphism $\pi\colon L \to (L + N)/N$ given by $\pi(x) = x + N$.]

Solution: Let π be as described. Every element of $(L + N)/N$ has the form $z + N$ for some $z \in L + N$. We can write z as $x + y$ for some $x \in L$ and $y \in N$, so $z + N = x + y + N = x + N$

(because $y+N=N$). Thus every element of $(L+N)/N$ has the form $\pi(x)$ for some $x \in L$, which means that π is surjective.

Next, $\ker(\pi)$ is the set of those $x \in L$ for which $x+N=N$, or in other words those $x \in L$ for which we also have $x \in N$, so $\ker(\pi) = L \cap N$.

The First Isomorphism Theorem now tells us that

$$L/(L \cap N) = L/\ker(\pi) \simeq \text{image}(\pi) = (L+N)/N.$$

Q30: Let M be a module over a ring R, and let N_0 and N_1 be submodules of M. Define a homomorphism $\sigma\colon N_0 \oplus N_1 \to M$ by $\sigma(n_0, n_1) = n_0 + n_1$. Prove that σ is an isomorphism if and only if M is the internal direct sum of N_0 and N_1.

Solution: The homomorphism σ is an isomorphism iff it is both injective and surjective, or equivalently $\ker(\sigma) = \{0\}$ and $\text{image}(\sigma) = M$. We have $\text{image}(\sigma) = M$ iff every element of M can be written in the form $n_0 + n_1$ for some $n_0 \in N_0$ and $n_1 \in N_1$, or equivalently $M = N_0 + N_1$. Next, $\ker(\sigma)$ is the set of pairs $(n, -n)$ where $n \in N_0$ and $-n \in N_1$. However, we have $-n \in N_1$ iff $n \in N_1$, so $\ker(\sigma) = \{(n,-n) \mid n \in N_0 \cap N_1\}$. It follows that $\ker(\sigma) = \{0\}$ iff $N_0 \cap N_1 = \{0\}$. Thus σ is an isomorphism iff $M = N_0 + N_1$ and $N_0 \cap N_1 = \{0\}$, which means precisely that M is the internal direct sum of N_0 and N_1.

7. Ideals and factor rings

Q31:

(a) Show that there are no ring homomorphisms from $\mathbb{Z}_3$ to $\mathbb{Z}$. [Consider the equation $\overline{1}+\overline{1}+\overline{1} = \overline{0}$].

(b) Show that there are no ring homomorphisms from $\mathbb{Q}$ to $\mathbb{Z}$. [Consider the equation $\frac{1}{2}.(1+1) = 1$.]

(c) Show that there are no ring homomorphisms from $\mathbb{C}$ to $\mathbb{R}$.

(d) Find a ring homomorphism from $\mathbb{C}$ to $\mathbb{C}$ that is not the identity (there is only one reasonable example).

Solution:

(a) Let α be a ring homomorphism from $\mathbb{Z}_3$ to $\mathbb{Z}$. By applying α to the equation $\overline{1}+\overline{1}+\overline{1} = \overline{0}$ we obtain $\alpha(\overline{1}) + \alpha(\overline{1}) + \alpha(\overline{1}) = \alpha(\overline{0})$ but $\alpha(\overline{1}) = 1$ and $\alpha(\overline{0}) = 0$ so $1+1+1 = 0$ in $\mathbb{Z}$. This is clearly false, so no such α can exist.

(b) Let α be a ring homomorphism from $\mathbb{Q}$ to $\mathbb{Z}$. By applying α to the equation $\frac{1}{2}.(1+1) = 1$ we get $\alpha(\frac{1}{2}).(\alpha(1) + \alpha(1)) = \alpha(1)$. We also have $\alpha(1) = 1$ so $\alpha(\frac{1}{2}).2 = 1$. However, there is no element $x \in \mathbb{Z}$ with $x.2 = 1$ so this is impossible, so no such α can exist.

(c) Let α be a ring homomorphism from $\mathbb{C}$ to $\mathbb{R}$. By applying α to the equation $i^2 + 1 = 0$ we obtain $\alpha(i)^2 + \alpha(1) = \alpha(0)$ or in other words $\alpha(i)^2 + 1 = 0$. There is no element $x \in \mathbb{R}$ with $x^2 + 1 = 0$, so this is impossible, so no such α can exist.

(d) The only reasonable example is given by $\alpha(z) = \overline{z}$ (the complex conjugate of z). This is a ring homomorphism because $\overline{z+w} = \overline{z} + \overline{w}$ and $\overline{zw} = \overline{z}\,\overline{w}$ and $\overline{1} = 1$. (There are some other examples defined by a bizarre procedure involving heavy set theory. The above example is the only one that is a continuous function from $\mathbb{C}$ to itself.)

Q32:

(a) Prove that $\mathbb{Q}[x]/(x^2-2)$ is isomorphic to a subring of $\mathbb{R}$.

(b) Let I be the ideal $\mathbb{Z}[i].(2+3i)$ in $\mathbb{Z}[i]$, and define a homomorphism $\alpha\colon \mathbb{Z} \to \mathbb{Z}[i]/I$ by $\alpha(n) = n + I$.

(i) Show that $\alpha(-5) = i + I$, and deduce that α is surjective.

(ii) Suppose that $n \in \mathbb{Z}$ and that n is divisible by $2+3i$ in $\mathbb{Z}[i]$. Show that n^2 is divisible by 13 in $\mathbb{Z}$.

(iii) Show that $\mathbb{Z}[i]/I \simeq \mathbb{Z}_{13}$.

Solution:

(a) Define $\alpha\colon \mathbb{Q}[x] \to \mathbb{R}$ by $\alpha(f) = f(\sqrt{2})$; this is clearly a ring homomorphism. As $(\sqrt{2})^2 - 2 = 0$ we have $x^2 - 2 \in \ker(\alpha)$, so $\mathbb{Q}[x].(x^2-2) \subseteq \ker(\alpha)$. Conversely, suppose that $f \in \ker(\alpha)$, so $f(\sqrt{2}) = 0$. We can divide $f(x)$ by x^2-2 to get $f(x) = (x^2-2)q(x) + a + bx$ for some $a, b \in \mathbb{Q}$. We then have

$$0 = f(\sqrt{2}) = (\sqrt{2}^2 - 2)q(\sqrt{2}) + a + b\sqrt{2} = a + b\sqrt{2}.$$

If $b \neq 0$ we can deduce that $\sqrt{2} = -a/b$ which is impossible as $\sqrt{2}$ is irrational. Thus, we must have $b = 0$, in which case the equation $0 = a + b\sqrt{2}$ tells us that $a = 0$ also. Thus $f(x) = (x^2-2)q(x)$, so $f(x) \in \mathbb{Q}[x].(x^2-2)$. Thus $\ker(\alpha) = \mathbb{Q}[x].(x^2-2)$, so $\mathbb{Q}[x]/(x^2-2) \simeq \text{image}(\alpha)$ (by the First Isomorphism Theorem for rings), and $\text{image}(\alpha)$ is a subring of $\mathbb{R}$ as required.

(b) (i) We have $\alpha(-5) = -5 + I$, and we want to show that this is the same as $i + I$, or in other words that $-5 - i \in I$. By direct calculation we have $(-5-i)/(2+3i) = 1+i$ which lies in $\mathbb{Z}[i]$, so $-5 - i = (1+i)(2+3i) \in \mathbb{Z}[i].(2+3i) = I$ as required.
Now suppose we have an element $a + ib + I \in \mathbb{Z}[i]/I$ (so $a, b \in \mathbb{Z}$). We find that $\alpha(a - 5b) = \alpha(a) + \alpha(b)\alpha(-5) = a + bi + I$, and it follows that α is surjective.

(ii) Suppose that $n = (2+3i)(u+iv)$. By taking norms we find that $n^2 = N(n) = N(2+3i)N(u+iv) = 13(u^2+v^2)$, so n^2 is divisible by 13 in $\mathbb{Z}$.

(iii) As $13 = (2+3i)(2-3i) \in I$ we have $\alpha(13) = 0$ so $13\mathbb{Z} \subseteq \ker(\alpha)$. Conversely, suppose that $\alpha(n) = 0$, so n is divisible by $2+3i$ in $\mathbb{Z}[i]$. By (ii) we see that n^2 is divisible by 13, but 13 is prime so n itself must be divisible by 13, so $n \in 13\mathbb{Z}$. Thus $\ker(\alpha) = 13\mathbb{Z}$ and $\mathbb{Z}_{13} = \mathbb{Z}/13\mathbb{Z} \simeq \text{image}(\alpha) = \mathbb{Z}[i]/I$.

Q33:

(a) Prove that the ring $\mathbb{R}[x]/(x^2+4)$ is isomorphic to $\mathbb{C}$.

(b) Prove that $\mathbb{R}[x]/(x^2-4)$ is not a field (and thus cannot be isomorphic to $\mathbb{C}$).

Solution:

(a) Define $\alpha\colon \mathbb{R}[x] \to \mathbb{C}$ by $\alpha(f) = f(2i)$. This is clearly a ring homomorphism. Any complex number $a + ib$ can be written as $\alpha(a + bx/2)$, so α is surjective. Put

$$I = \ker(\alpha) = \{f \in \mathbb{R}[x] \mid f(2i) = 0\}.$$

The First Isomorphism Theorem for rings now tells us that $\mathbb{R}[x]/I \simeq \mathbb{C}$, so it will be enough to show that $I = \mathbb{R}[x].(x^2+4)$. It is clear that the polynomial $f(x) = x^2+4$ satisfies $f(2i) = 0$, so $x^2 + 4 \in I$, so $\mathbb{R}[x].(x^2+4) \subseteq I$.

Conversely, suppose that $g(x) \in I$, so $g(2i) = 0$. By the division algorithm we have $g(x) = q(x)(x^2+4) + ax + b$ for some polynomial $q(x) \in \mathbb{R}[x]$ and some $a, b \in \mathbb{R}$. If we substitute $x = 2i$ in this relation and use the fact that $g(2i) = 0$ we find that $2ai + b = 0$. As a and b are real, we can conclude that $a = b = 0$, so $g(x) = q(x)(x^2+4)$, so $g(x) \in \mathbb{R}[x].(x^2+4)$. Thus $I = \mathbb{R}[x].(x^2+4)$, as required.

(b) In $\mathbb{R}[x]/(x^2-4)$ the elements $\overline{x-2}$ and $\overline{x+2}$ are nonzero, but their product is $\overline{x^2-4} = \overline{0}$. Thus $\mathbb{R}[x]/(x^2-4)$ is not an integral domain, and thus not a field.

Q34: Let R be the ring $\mathbb{Z}[i]/3$, and put $u = 1 + i + 3\mathbb{Z}[i] \in R$.

(a) List the elements of R.

(b) Calculate u^k for $0 \leq k \leq 8$.

(c) Compare your list in (a) with your list in (b), and show that R is a field.

(d) Do you know another proof that R is a field?

Solution:

(a) I claim that

$$R = \{\overline{0}, \overline{1}, \overline{2}, \overline{i}, \overline{1+i}, \overline{2+i}, \overline{2i}, \overline{1+2i}, \overline{2+2i}\},$$

or equivalently $R = \{\overline{a+bi} \mid a, b \in \{0,1,2\}\}$. Indeed, the listed elements are certainly contained in R, and it is easy to see that they are all different. Conversely, any element $x \in R$ can be written as $x = \overline{a+ib}$ for some $a, b \in \mathbb{Z}$. We can then write $a = 3c + a'$ for some $c \in \mathbb{Z}$ and $a' \in \{0,1,2\}$ and $c \in \mathbb{Z}$. Similarly we have $b = 3d + b'$ for some $d \in \mathbb{Z}$ and $b' \in \{0,1,2\}$. It follows that $(a+bi) = (a'+b'i) + 3(c+di)$, so $x = \overline{a'+b'i}$, so x is in our list.

(b) Here we will just write $a+bi$ for $\overline{a+bi}$. We have

$$\begin{aligned}
u^0 &= 1 \\
u^1 &= 1+i \\
u^2 &= (1+i)^2 = 2i \\
u^3 &= u^2.u = 2i(1+i) = 2i - 2 = 2i + 1 \\
u^4 &= (u^2)^2 = -4 = 2 \\
u^5 &= u^4.u = 2 + 2i \\
u^6 &= u^4.u^2 = 4i = i \\
u^7 &= u^4.u^3 = 4i + 2 = i + 2 \\
u^8 &= (u^4)^2 = 4 = 1.
\end{aligned}$$

(c) On comparing (a) with (b) we see that every nonzero element of R is a power of u. We also have $u^8 = 1$, so u^{8-k} is an inverse for u^k, so every nonzero element of the ring R is invertible. This means that R is a field.

(d) If we can prove that 3 is irreducible in $\mathbb{Z}[i]$, it will follow that $\mathbb{Z}[i]/3$ is a field (Proposition 10.6 in the notes). It is a general fact that prime numbers of the form $4k-1$ are irreducible in $\mathbb{Z}[i]$, and this obviously covers the case of the prime 3. More explicitly, if 3 were reducible we would have $3 = rs$ for some nonunits r and s. We would then have $9 = N(3) = N(r)N(s)$, and $N(r), N(s) \neq 1$ as r and s are not units. This means we must have $N(r) = N(s) = 3$. However, 3 cannot be written as $a^2 + b^2$ for any integers a and b, so we cannot have $N(r) = 3$, so 3 must be irreducible after all.

8. Euclidean domains

Q35: Let n and m be coprime positive integers, and put $f(x) = x^n - 1$ and $g(x) = x^m - 1$. By considering the roots of f and g, show that the gcd of f and g in $\mathbb{C}[x]$ is $x - 1$.

Solution: Let h be the gcd of f and g, which we can take to be monic. Note that $f(1) = g(1) = 0$, so both f and g are divisible by $x-1$, so h is divisible by $x-1$, or equivalently $h(1) = 0$. We claim that this is the only root of h. Indeed, suppose that $h(\zeta) = 0$. As h divides both f and g and $h(\zeta) = 0$, we see that $f(\zeta) = g(\zeta) = 0$, so $\zeta^n = \zeta^m = 1$. We are also given that n and m are coprime, so $nu + mv = 1$ for some integers u and v. We deduce that

$$\zeta = \zeta^1 = \zeta^{nu+mv} = (\zeta^n)^u (\zeta^m)^v = 1^u 1^v = 1,$$

so $\zeta = 1$ as claimed. As this is the only root of h, we see that $h(x) = (x-1)^k$ for some $k > 0$. To show that $k = 1$, it will suffice to check that f and g are not divisible by $(x-1)^2$, or equivalently that $f'(1) \neq 0 \neq g'(1)$. This is clear from the formulae: we have $f'(x) = nx^{n-1}$, so $f'(1) = n > 0$, and similarly $g'(1) = m > 0$.

Q36: Let p be a prime, and let a and b be nonzero elements of $\mathbb{Z}_{(p)}$. Show that either a is a gcd of a and b in $\mathbb{Z}_{(p)}$, or b is a gcd of a and b in $\mathbb{Z}_{(p)}$.

Solution: We can write $a = p^n r/s$ for some integer $n \geq 0$ and some integers r, s that are not divisible by p. Similarly, we can write $b = p^m t/u$ for some integer $m \geq 0$ and some integers t, u that are not divisible by p. If $n \leq m$ then the number $x = b/a = p^{m-n}ts/ru$ lies in $\mathbb{Z}_{(p)}$ and $b = ax$. This says that b is divisible by a, and it follows easily that a is a gcd of a and b. Similarly, if $n \geq m$ then b is a gcd of a and b.

9. Finite free modules over a Euclidean domain

Q37: Find bases over $\mathbb{Z}$ for the following submodules of $\mathbb{Z}^3$. Justify your answers.

(a) $M_0 = \{(x, y, z) \mid x - y + z = 0 \pmod 5\}$
(b) $M_1 = \{(x, y, z) \mid x = y \pmod 2 \text{ and } y = z \pmod 3\}$
(c) $M_2 = \{(x, y, z) \mid 6x + 15y + 10z = 0\}$.

Solution:

(a) Put $u = (1, 1, 0)$ and $v = (0, 1, 1)$ and $w = (0, 0, 5)$. I claim that these vectors form a basis for M_0 over $\mathbb{Z}$. Indeed, it is easy to see that u, v and w all lie in M_0. Moreover, if $m = (x, y, z) \in M_0$ then $x - y + z = 5t$ for some t, so $z = 5t - x + y$, and one checks that

$$\begin{aligned} xu + (y - x)v + tw &= (x, x, 0) + (0, y - x, y - x) + (0, 0, 5t) \\ &= (x, y, 5t + y - x) = (x, y, z) = m. \end{aligned}$$

This shows that m lies in the submodule generated by u, v and w, and it is clear that u, v and w are linearly independent over $\mathbb{Z}$, so they form a basis as claimed.

(b) Here we put $u = (2, 0, 0)$ and $v = (3, 3, 0)$ and $w = (1, 1, 1)$; these are easily seen to be elements of M_1. Given an arbitrary element $m = (x, y, z) \in M_1$, we note that $x - y = 2s$ and $y - z = 3t$ for some integers s, t. It follows that

$$\begin{aligned} su + tv + zw &= (2s, 0, 0) + (3t, 3t, 0) + (z, z, z) \\ &= (x - y, 0, 0) + (y - z, y - z, 0) + (z, z, z) \\ &= (x, y, z) = m. \end{aligned}$$

This shows that m lies in the submodule generated by u, v and w, and it is clear that u, v and w are linearly independent over $\mathbb{Z}$, so they form a basis as claimed.

(c) Here we put $u = (5, -2, 0)$ and $v = (0, 2, -3)$; these are easily seen to be elements of M_2. Now consider an arbitrary element $m = (x, y, z) \in M_2$, so $6x + 15y + 10z = 0$. We can reduce this equation modulo 5: as $6x = x \pmod 5$ and $15y = 10z = 0 \pmod 5$, we deduce that $x = 0 \pmod 5$. Similarly, we can reduce modulo 2 to show that $y = 0 \pmod 2$, and reduce mod 3 to see that $z = 0 \pmod 3$. We thus have $(x, y, z) = (5r, 2s, 3t)$ for some $r, s, t \in \mathbb{Z}$. The equation $6x + 15y + 10z = 0$ now gives $30r + 30s + 30t = 0$, so $r + s + t = 0$. It follows that

$$\begin{aligned} ru - tv &= (5r, -2r, 0) - (0, 2t, -3t) \\ &= (5r, -2(t + r), 3t) \\ &= (5r, 2s, 3t) = (x, y, z) = m. \end{aligned}$$

This shows that m lies in the submodule generated by u and v, and it is clear that u, v and w are linearly independent over $\mathbb{Z}$, so they form a basis as claimed.

Q38: Let $d_1, \ldots, d_n$ be elements of a ring R, and let N be the submodule of R^n generated by the elements $d_1 e_1, \ldots, d_n e_n$. Prove that $R^n/N \simeq R/d_1 \oplus \ldots \oplus R/d_n$. [You may wish to start by defining a homomorphism $\alpha\colon R^n \to R/d_1 \oplus \ldots \oplus R/d_n$.]

Solution: We can define $\alpha : R^n \to R/d_1 \oplus \ldots \oplus R/d_n$ by

$$\alpha(a_1, \ldots, a_n) = (a_1 + Rd_1, \ldots, a_n + Rd_n).$$

Suppose we have an element $(u_1, \ldots, u_n) \in R/d_1 \oplus \ldots \oplus R/d_n$, so $u_i \in R/d_i$ for $i = 1, \ldots, n$. For each i we can choose $a_i \in R$ such that $u_i = a_i + Rd_i$, and then $\alpha(a_1, \ldots, a_n) = (u_1, \ldots, u_n)$. Thus α is surjective, and the First Isomorphism Theorem now tells us that $R^n/\ker(\alpha) \simeq R/d_1 \oplus \ldots \oplus R/d_n$. We now need to determine the kernel of α. If $\alpha(a_1, \ldots, a_n) = 0$ then $a_i + Rd_i$ must be the zero element of R/d_i for all i. This means that $a_i \in Rd_i$, so $a_i = b_i d_i$ say. It follows that $\underline{a} = \sum_i a_i e_i = \sum_i b_i.(d_i e_i) \in N$. Conversely, it is clear that $\alpha(d_i e_i) = 0$ for all i, so that $N \subseteq \ker(\alpha)$, so $\ker(\alpha) = N$. Thus $R^n/N \simeq R/d_1 \oplus \ldots \oplus R/d_n$ as claimed.

Q39: Put

$$F = \{(w, x, y, z) \in \mathbb{Z}^4 \mid w + x + y + z \text{ is even } \}$$
$$G = \{(w, x, y, z) \in \mathbb{Z}^4 \mid w - x,\ x - y, \text{ and } y - z \text{ are divisible by } 4\}.$$

Find integers $d_1, d_2, d_3, d_4 > 0$ and vectors $u_1, u_2, u_3, u_4 \in \mathbb{Z}^4$ such that $\{u_1, u_2, u_3, u_4\}$ is a basis for F and $\{d_1 u_1, d_2 u_2, d_3 u_3, d_4 u_4\}$ is a basis for G. [It is possible to do this using matrix methods, but intelligent trial and error is likely to be easier.] It follows that $G \subseteq F$, so we can form the factor group F/G. Deduce a description of F/G as a direct sum of cyclic groups.

Solution: One solution is as follows:

$$u_1 = (1, 1, 1, 1) \qquad d_1 = 1$$
$$u_2 = (0, 0, 0, 2) \qquad d_1 = 2$$
$$u_3 = (0, 1, 1, 0) \qquad d_1 = 4$$
$$u_4 = (0, 0, 1, 1) \qquad d_1 = 4.$$

Put $v_i = d_i u_i$. It is clear that the set $\{u_1, \ldots, u_4\}$ is linearly independent, as is the set $\{v_1, \ldots, v_4\}$. It will thus be enough to show that the elements u_i generate F, and the elements v_i generate G.

It is clear that the elements u_i all lie in F. Suppose we have an element $f = (w, x, y, z) \in F$, so $w + x + y + z = 2t$ for some integer t. We then have

$$\begin{aligned} wu_1 + (t - w - x)u_2 + (x - w)u_3 + (y - x)u_4 &= (w, w, w, w) + (0, 0, 0, 2t - 2w - 2x) + \\ &\quad (0, x - w, x - w, 0) + (0, 0, y - x, y - x) \\ &= (w, x, y, 2t - w - x - y) = (w, x, y, z). \end{aligned}$$

Thus f lies in the $\mathbb{Z}$-submodule generated by $\{u_1, \ldots, u_4\}$, as required.

Next, we have

$$v_1 = (1, 1, 1, 1)$$
$$v_2 = (0, 0, 0, 4)$$
$$v_3 = (0, 4, 4, 0)$$
$$v_4 = (0, 0, 4, 4).$$

These vectors clearly lie in G. Suppose we have an element $g = (w, x, y, z) \in G$, so $w - x = 4r$, $x - y = 4s$ and $y - z = 4t$ for some integers r, s, t. We then have $x = w - 4r$ and $y = x - 4s = w - 4r - 4s$ and $z = y - 4t = w - 4r - 4s - 4t$, so $g = (w, w - 4r, w - 4r - 4s, w - 4r - 4s - 4t)$. From this we see directly that $g = wv_1 - (t + r)v_2 + rv_3 + sv_4$. Thus f lies in the $\mathbb{Z}$-submodule generated by $\{u_1, \ldots, u_4\}$, as required.

We now deduce that

$$\frac{F}{G} \simeq \frac{\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}}{\mathbb{Z} \oplus 2\mathbb{Z} \oplus 4\mathbb{Z} \oplus 4\mathbb{Z}} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4.$$