Fields, rings, and modules
Exercise sheet 5

https://www.maths.tcd.ie/~mascotn/teaching/2021/MAU22102/index.html

Version: April 20, 2021

Email your answers to aylwarde@tcd.ie by Monday April 19, 4PM.

Exercise 1 *A non-free module over a non-commutative ring (50 pts)*

Let $M_2 = M_2(\mathbb{R})$ be the ring of 2×2 matrices with real entries, and let $V = \mathbb{R}^2$ be the space of column vectors of size 2 with real entries.

1. (20 pts) Prove that the natural multiplication $M_2 \times V \longrightarrow V$ gives V the structure of an M_2-module (so that the elements of V are the "vectors" and the elements of M_2 are the "scalars").

2. (15 pts) Find a generating set for the M_2-module V containing as few elements as possible.

3. (15 pts) Prove that V is **not** a free M_2-module.

   Hint: Consider the dimensions of the underlying $\mathbb{R}$-vector spaces.

Solution 1

1. V is an $\mathbb{R}$-vector space, so in particular it already has an addition law

$$V \times V \longrightarrow V$$

   giving it an Abelian group structure. Define an external multiplication on V by

$$\begin{array}{ccc} M_2 \times V & \longrightarrow & V \\ (A, v) & \longmapsto & Av, \end{array}$$

   which makes sense since we are viewing the elements of V as column vectors. Then V has the two operations required to be an M_2-module. It remains to check that the appropriate axioms hold:

   - We do have $(AB)v = A(Bv)$ for all $A, B \in M_2$ and $v \in V$,
   - The 1 of the ring M_2 is the identity matrix 1_2, and we do have $1_2 v = v$ for all $v \in V$,
   - We do have $A(v + w) = Av + Aw$ for all $A \in M_2$ and $v, w \in V$,
   - And finally, we do have $(A+B)v = Av+Bv$ for all $A, B \in M_2$ and $v \in V$.

2. Let $v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in V$. Then $\{v_1\} \subset V$ generates V as an M_2 module. Indeed, any $v = \begin{pmatrix} x \\ y \end{pmatrix} \in V$ is of the form $v = Av_1$ for some $A \in M_2$, namely any A having v as a first column (i.e. of the form $A = \begin{pmatrix} x & * \\ y & * \end{pmatrix}$, where $*$ can be anything). Besides, this generating set is clearly minimal (i.e. has as few elements as possible) since the empty set generates the submodule $\{0\} \subsetneq V$.

3. CAUTION THERE! One can check that $\{v_1\}$ is not linearly independent (because we have the nontrivial linear dependency relation $Av_1 = 0$ for $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq 0$ for instance), BUT this does not constitute a proof since we do not have any statement saying that if V were free then we could extract a basis out of the generating set $\{v_1\}$ — this does not hold for modules! So we must take another approach.

   Suppose by contradiction that V is a free M_2-module of rank n, so that we have an isomorphism $f : V \simeq M_2^n$ of M_2-modules. Let us prove that f is also an isomorphism of $\mathbb{R}$-vector spaces. We have $f(v+w) = f(v) + f(w)$ for all $v, w \in V$ since f is a module morphism, and if we set $A_\lambda = \lambda 1_2$ for $\lambda \in \mathbb{R}$, then we have

   $$f(\lambda v) = f(A_\lambda v) = A_\lambda f(v) = \lambda f(v)$$

   for all $\lambda \in \mathbb{R}$ and $v \in V$, where we have used the M_2-linearity of f at the second step. So f is $\mathbb{R}$-linear. Since f is also bijective, it is an isomorphism of $\mathbb{R}$-vector spaces. Therefore, $V \simeq M_2^n$ as $\mathbb{R}$-vector spaces. But the LHS has dimension 2 over $\mathbb{R}$, whereas the RHS has dimension $4n$. Since 2 is not of the form $4n$, we have a contradiction.

Exercise 2 *Finitely generated Abelian groups (50 pts)*

1. (20 pts) Let G be the Abelian group with generators g, h and relations $8g + 12h = 6g + 8h = 0$. Perform an SNF computation to determine what G is isomorphic to.

2. (15 pts) Determine $\#G$. Is G cyclic?

3. (15 pts) Find all Abelian groups of order 2020, up to isomorphism.

Solution 2

1. We must determine the SNF of

   $$A = \begin{pmatrix} 8 & 6 \\ 12 & 8 \end{pmatrix}$$

   over $\mathbb{Z}$. The smallest entry is 6, so $C_2 \leftrightarrow C_1$:

   $$\begin{pmatrix} 6 & 8 \\ 8 & 12 \end{pmatrix}$$

Then we use 6 as a pivot, so $R_2 \leftarrow R_2 - R_1$ then $C_2 \leftarrow C_2 - C_1$ (the other way round is also OK):

$$\begin{pmatrix} 6 & 2 \\ 2 & 2 \end{pmatrix}$$

We do not yet have zeros at the top-right and bottom-left, so we move one of the smallest entries (a 2) to the top-left, e.g. $R_2 \leftrightarrow R_1$:

$$\begin{pmatrix} 2 & 2 \\ 6 & 2 \end{pmatrix}$$

and we use that 2 as a pivot: $R_2 \leftarrow R_2 - 3R_1$ then $C_2 \leftarrow C_2 - C_1$ (the other way round is also OK):

$$\begin{pmatrix} 2 & 0 \\ 0 & -4 \end{pmatrix}$$

This is a diagonal matrix ad $2 \mid -4$, so this is our SNF. Thus

$$G \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/-4\mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$$

as $-4\mathbb{Z} = 4\mathbb{Z}$ (namely, -4 and 4 are associates in $\mathbb{Z}$).

2. Since $G \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$, we have $\#G = 2 \times 4 = 8$. If G were cyclic, we would have $G \simeq \mathbb{Z}/8\mathbb{Z}$; however the invariant factors

$$2 \mid 4$$

and

$$8$$

are NOT the same up to associates, so

$$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z}) \not\simeq (\mathbb{Z}/8\mathbb{Z});$$

thus G is not NOT cyclic. (Alternative proof: $\mathbb{Z}/8\mathbb{Z}$ has elements of order 8, but the order of an element of $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ is at most 4.)

3. Let H be an Abelian group of order $\#H = 2020$. Then H is finite, so finitely-generated (since it is clearly generated by all its elements!), so there are non-negative integers $d_1 \mid d_2 \mid \cdots$ such that

$$H \simeq (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \times \cdots ;$$

in particular $d_1 \times d_2 \times = 2020$. Since these invariant factors are unique, finding all such H up to isomorphism amounts fining all the $d_1 \mid d_2 \mid \cdots$ such that $d_1 \times d_2 \times = 2020$. As 2020 factors as

$$2020 = 2^2 \times 5 \times 101$$

and 101 is prime, we only have two possibilities:

$$d_1 = 2,\ d_2 = 1010$$

and

$$d_1 = 2020$$

(since $d_2 \mid d_1$ implies $d_2^2 \mid d_1 d_2 \cdots = 2020$). So up to isomorphism, the only such groups are

$$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/1010\mathbb{Z})$$

(which is not cyclic), and

$$(\mathbb{Z}/2020\mathbb{Z})$$

(which is cyclic).

These were the only mandatory exercises, that you must submit before the deadline. The following exercise is not mandatory; it is not worth any points, and you do not have to submit them. However, you can try to solve them for practice, and you are welcome to email me if you have questions about them. The solutions will be made available with the solution to the mandatory exercises.

Exercise 3 *A very algebraic viewpoint on modules*

In this exercise, whenever G is an Abelian group, we write $\mathrm{End}(G)$ for the set of group morphisms from G to itself, and we equip this set with the addition defined by

$$\forall f, g \in \mathrm{End}(G),\ \forall x \in G,\ (f+g)(x) \stackrel{\text{def}}{=} f(x) + g(x)$$

and with the multiplication defined by

$$\forall f, g \in \mathrm{End}(G),\ \forall x \in G,\ (f \times g)(x) \stackrel{\text{def}}{=} f(g(x)).$$

In other words, addition in $\mathrm{End}(G)$ means pointwise addition, and multiplication in $\mathrm{End}(G)$ means composition.

1. Let G be an Abelian group. Prove that the addition and the multiplication in $\mathrm{End}(G)$ defined above define a (not necessarily commutative) ring structure on $\mathrm{End}(G)$. What are its 0, and its 1?

2. Let R be a ring, and let M be an R-module. Then M is in particular an Abelian group, so we can define $\mathrm{End}(M)$ and put a ring structure on it as in the previous question. In other words, $\mathrm{End}(M)$ is the ring of Abelian group morphisms (as opposed to module morphisms) form M to itself.

   (a) Fix $\lambda \in R$, and denote by μ_λ (standing for "multiplication by λ") the map

   $$\begin{array}{rccc} \mu_\lambda : & M & \longrightarrow & M \\ & m & \longmapsto & \lambda m. \end{array}$$

   Prove that $\mu_\lambda \in \mathrm{End}(M)$.

   (b) Prove that the map

   $$\begin{array}{rccc} \mu : & R & \longrightarrow & \mathrm{End}(M) \\ & \lambda & \longmapsto & \mu_\lambda \end{array}$$

   is a ring morphism.

3. Conversely, given an Abelian group G and a ring R, prove that assigning a ring morphism $\mu : R \longrightarrow \mathrm{End}(G)$ equips G with an R-module structure.

Solution 3

1. First of all, one checks easily that if $f, g \in \mathrm{End}(G)$, then $f+g$ and $fg \in \mathrm{End}(G)$. Next, since $(G,+)$ is an Abelian group, $(\mathrm{End}(G),+)$ is also an Abelian group; its identity is the 0 map, which does lie in $\mathrm{End}(G)$, and the inverse of any $f \in \mathrm{End}(G)$ is $-f : x \mapsto -f(x)$, which does lie in $\mathrm{End}(G)$.

   Besides, it is clear that multiplication is associative in $\mathrm{End}(G)$, and that the identity map $\mathrm{Id} : x \mapsto x$, which does lie in $\mathrm{End}(G)$, is a neutral element for multiplication.

   It remains to check distributivity. Let $f, g, h \in \mathrm{End}(G)$, and let $x \in G$; then

$$\big(f(g+h)\big)(x) = f((g+h)(x)) = f(g(x)+h(x))$$

$$= f(g(x)) + f(h(x)) = (fg)(x) + (fh)(x) = (fg+fh)(x)$$

   and

$$\big((f+g)h\big)(x) = (f+g)(h(x)) = f(h(x))+g(h(x)) = (fh)(x)+(gh)(x) = (fh+gh)(x).$$

   Since this holds for all $x \in G$, we deduce that $f(g+h) = fg+fh$ and that $(f+g)h = fh+gh$, that is to say distributivity holds.

   This completes the proof that $\mathrm{End}(G)$ equipped with these laws is a ring, and we hve also proved that its 0 is the 0 map whereas its 1 is the identity map.

2. (a) Since M is an R-module, for all $m, n \in M$ we have

$$\lambda(m+n) = \lambda m + \lambda n,$$

   which means precisely that

$$\mu_\lambda(m+n) = \mu_\lambda(m) + \mu_\lambda(n).$$

   Since this holds for all $m, n \in M$, this proves that $\mu_\lambda \in \mathrm{End}(M)$.

   (b) Let $\lambda, \lambda' \in R$. Then for all $m \in M$, we have

$$\mu_{\lambda+\lambda'}(m) = (\lambda+\lambda')m = \lambda m + \lambda' m = \mu_\lambda(m) + \mu_{\lambda'}(m) = (\mu_\lambda + \mu_{\lambda'})(m),$$

   so that $\mu_{\lambda+\lambda'} = \mu_\lambda + \mu_{\lambda'}$,

$$\mu_{\lambda\lambda'}(m) = (\lambda\lambda')m = \lambda(\lambda' m) = \mu_\lambda(\mu_{\lambda'}(m)) = (\mu_\lambda \mu_{\lambda'})(m),$$

   so that $\mu_{\lambda\lambda'} = \mu_\lambda \mu_{\lambda'}$, and finally

$$\mu_1(m) = 1m = m = \mathrm{Id}(m) = 1_{\mathrm{End}(M)}(m)$$

   so $\mu_1 = 1_{\mathrm{End}(M)}$. Thus $\lambda \mapsto \mu_\lambda$ is a ring morphism.

3. Let us define a multiplication of R on G by the rule

$$rg = \mu(r)(g) \qquad (r \in \mathbb{R}, g \in G),$$

   and prove that this makes G an R-module.

We already have that M is an Abelian group. Besides, since μ assumes values in $\mathrm{End}(G)$, we have that for all $r \in R$ and $g, h \in G$,

$$r(g+h) = \mu(r)(g+h) = \mu(r)(g) + \mu(r)(h) = rg + rh.$$

Finally, since μ is a ring morphism, we have $\mu(r+s) = \mu(r) + \mu(s)$, $\mu(rs) = \mu(r)\mu(s)$ for all $r, s \in R$, and $\mu(1) = 1_{\mathrm{End}(G)} = \mathrm{Id}$, so

$$(r+s)(g) = \mu(r+s)(g) = \mu(r)(g) + \mu(s)(g) = rg + sg,$$

$$(rs)(g) = \mu(rs)(g) = \mu(r)(g)(\mu(s)(g)) = r(sg),$$

and

$$1g = \mu(1)(g) = \mathrm{Id}(g) = g$$

for all $g \in G$. This completes the proof that μ gives G an R-module structure.

Note: The upshot of this exercise is that endowing G with an R-module structure amounts to specifying a ring morphism from R to $\mathrm{End}(G)$.