7210 HW 10

Duncan Wilkie

15 November 2022

Problem 1 (D&F 10.1.8)**.** *An element m of the R-module M is called a **torsion element** if $rm = 0$ for some nonzero element $r \in R$. The set of torsion elements is denoted*

$$\mathrm{Tor}(M) = \{m \in M \mid rm = 0 \textit{ for some nonzero } r \in R\}$$

1. *Prove that if R is an integral domain then $\mathrm{Tor}(M)$ is a submodule of M (called the **torsion** submodule of M).*
2. *Give an example of a ring R and an R-module M such that $\mathrm{Tor}(M)$ is not a submodule.*
3. *Show that if R has zero divisors then every nonzero R-module has torsion elements.*

Proof. We must prove that $\mathrm{Tor}(M)$ is an additive subgroup closed under the action of ring elements: if $rm = 0$ and $sn = 0$ for $m, n \in M$ and nonzero $r, s \in R$, then $rs \neq 0$ since this is an integral domain, and

$$(rs)(m - n) = s(rm) - r(sn) = s(0) - r(0) = 0 \Rightarrow m - n \in \mathrm{Tor}(M).$$

The additive identity is certainly an element of $\mathrm{Tor}(M)$. Further, if $rm = 0$ for some nonzero $r \in R$ then for all nonzero $s \in R$ one has that

$$r(sm) = s(rm) = s(0) = 0 \Rightarrow sm \in \mathrm{Tor}(M).$$

This proves $\mathrm{Tor}(M)$ is a submodule.

Consider $\mathbb{Z}/6\mathbb{Z}$ as a module over itself. The residue classes 2 and 3 are zero divisors: they multiply to the zero residue class. The difference $3 - 2 = 1$, however, is not a zero divisor as it is the multiplicative identity; accordingly, the torsion of this module isn't closed under addition (note that the failure of the general argument is because $rs = 0$, since this fails to be an integral domain).

Suppose $rs = 0$ for nonzero $r, s \in R$ being zero divisors presumed to exist. Then for any element m of a module M over R one has

$$0 = 0m = (rs)m = r(sm)$$

so sm is a torsion element of M. □

Problem 2 (D&F 10.1.15)**.** *If M is a finite Abelian group then M is naturally a $\mathbb{Z}$-module. Can this action be extended to make M into a $\mathbb{Q}$-module?*

Proof. Consider a finite Abelian group G with a $\mathbb{Q}$-module action extending that of $\mathbb{Z}$. Then for any nonzero a the element $\frac{1}{|G|}\cdot a$ has that the $|G|$-fold sum $\frac{1}{|G|}\cdot a+\cdots+\frac{1}{|G|}\cdot a$ equals 1, as $\frac{|G|}{|G|}\cdot a = 1\cdot a = a$ to agree with the $\mathbb{Z}$-action. No partial sum can be zero, as this would imply that some multiple of $\frac{1}{|G|}$ would be zero However, this implies that the order of 1 is more than $|G|$, which cannot happen. □

Problem 3 (D&F 10.2.6)**.** $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(n,m)\mathbb{Z}$.

Proof. Denote an element of the left ring by $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. Let φ be the map taking each ϕ to $\phi(1)$. This is a homomorphism out of the Hom-ring:

$$\varphi(\phi \circ \phi') = (\phi \circ \phi')(1) = \phi(\phi'(1)) = \phi(\phi'(1) \cdot 1) = \phi(1)\phi'(1) = \varphi(\phi)\varphi(\phi')$$

$$\varphi(\phi + \phi') = (\phi + \phi')(1) = \phi(1) + \phi'(1) = \varphi(\phi) + \varphi(\phi').$$

This is injective, since

$$\varphi(\phi) = \varphi(\phi') \Rightarrow \phi(1) = \phi'(1) \Rightarrow \phi(a) = \phi(a \cdot 1) = a\phi(1) = a\phi'(1) = \phi'(a);$$

concomitantly, its kernel is trivial, and the domain is isomorphic to the image of φ. This image is the whole of $\mathbb{Z}/(n,m)\mathbb{Z}$: each value of $\phi(1)$ specifies a distinct, valid homomorphism ϕ. □

Problem 4 (D&F 10.3.2)**.** *Assume R is commutative. Prove that $R^n \cong R^m$ iff $n = m$, i.e. two free R-modules of finite rank are isomorphic iff they have the same rank.*

Proof. If $n = m$, then the two are exactly equal, and isomorphic by the identity map. Suppose that $R^n \cong R^m$ by φ, and take I a maximal ideal in R. By exercise 12 in the previous section,

$$R^n/IR^n = \underbrace{R/IR \times R/IR \times \cdots \times R/IR}_{n \text{ times}}$$

and

$$R^m/IR^m = \underbrace{R/IR \times R/IR \times \cdots \times R/IR}_{m \text{ times}}$$

These two modules are isomorphic: $IR^m \cong IR^n$ by the map taking $\sum_{\text{finite}} a_i m_i$ to $\sum_{\text{finite}} a_i \varphi(m_i)$ where φ is the isomorphism between R^m and R^n (which is clearly an invertible module homomorphism by multiplicativity and invertibility of φ), and if the numerators and denominators are isomorphic, certainly the quotients are. For commutative rings as modules over themselves, ideals and quotients coincide as module- and ring-theoretic notions. Submodules are additive subgroups closed under multiplication on the left by arbitrary ring elements, and left ideals are two-sided in commutative rings; the quotient of modules is a quotient of Abelian groups with scalar multiplication defined on coset representatives satisfying the module identities, which induces a ring product on the cosets and vice versa, since all scalars represent some coset. The module R/IR considered as a ring is isomorphic to a field, and, accordingly, is module-isomorphic to a field acting on itself: the submodule IR is also a subring of R; as it's elements are of the form $\sum_{\text{finite}} a_i r_i$, and a_i are elements of I, a (two-sided) ideal, it equals I, and since I is maximal, the ring quotient yields a field. This proves that each of the products above is module-isomorphic to F^n and F^m. If these are module-isomorphic to each other, then $n = m$. □

Problem 5 (D&F 10.3.9). *An R-module M is called **irreducible** if $M \neq 0$ and if 0 and M are the only submodules of M. Show that M is irreducible iff $M \neq 0$ and M is a cyclic module with any nonzero element as a generator. Determine all the irreducible $\mathbb{Z}$-modules.*

Proof. Suppose M is irreducible. Then, it is generated by any element: if for some nonzero candidate $a \in M$ there is some element $m \in M$ such that $m \neq ra$, then Ra is a proper submodule of M.

Conversely, suppose M is cyclic with any nonzero element as a generator. Then, for any nonzero submodule N of M any nonzero element a of the submodule (which must exist!) generates M, so for all $m \in M$ one has $m = ra$ for some $r \in R$, and since N must be closed under scalar multiplication, this means $N = M$. This proves that M is irreducible.

We're looking for Abelian groups such that any nonzero element has that all elements are obtained as multiples of any of its elements. These are of course cyclic, so $\mathbb{Z}/n\mathbb{Z}$ for some n, but if n is composite, then its factors can't be obtained as multiples of each other, e.g. in $\mathbb{Z}/6\mathbb{Z}$, the multiples of 2 are 0, 2, 4 and the multiples of 3 are 0, 3. If n is prime, on the other hand, then $\mathbb{Z}/n\mathbb{Z}$ is a field and $ka \equiv b \pmod n$ is solvable for any b by inverting k. □

Problem 6 (D&F 12.1.2). *Let M be a module over the integral domain R.*

- *Suppose that M has rank n and that $x_1, x_2, \ldots, x_n$ is any maximal set of linearly independent elements of M. Let $N = Rx_1 + \cdots Rx_n$ be the submodule generated by $x_1, x_2, \ldots, x_n$. Prove that N is isomorphic to R^n and that the quotient M/N is a torsion R-module (equivalently, the elements $x_1, \ldots, x_n$ are linearly independent and for any $y \in M$ there is a nonzero element $r \in R$ such that ry can be written as a linear combination $r_1x_1 + \cdots + r_nx_n$ of the x_i).*
- *Prove conversely that if M contains a submodule N that is free of rank n (i.e., $N \cong R^n$) such that the quotient M/N is a torsion R-module then M has rank n.*

Proof. For every choice of $r_1, r_2, \ldots, r_n$ where at least one $r_i \neq 0$, one has $r_1x_1 + r_2x_2 + \cdots + r_nx_n \neq 0$. Accordingly, the value of the above sum is distinct for every selection of the r_i's, as if some other selection r_i' has the same value, then $(r_1 - r_1')x_1 + (r_2 - r_2')x_2 + \cdots + (r_n - r_n')x_n = 0$. As such, the map taking $(r_1, r_2, \ldots, r_n) \in R^n$ to $r_1x_1 + r_2x_2 + \cdots + r_nx_n \in N$ is injective; it is also surjective, since by definition N consists of all sums of this form. For any element $y \in M$, if there is no nonzero r such that one can write $ry = r_1x_1 + r_2x_2 + \cdots + r_nx_n$, then $x_1, x_2, \ldots, x_n, y$ is linearly independent by subtracting ry from both sides of the antecedent equation and noting existence of additive inverses.

Conversely, if M has a submodule N that is free of rank n such that M/N is a torsion R-module, then for any $y_1, y_2, \ldots, y_{n+1} \in M$ the fact that M/N is a torsion module means that any R-linear combination $r_1y_1 + r_2y_2 + \cdots + r_{n+1}y_{n+1}$ has that there exists some $r \neq 0$ such that $r(r_1y_1 + r_2y_2 + \cdots + r_{n+1}y_{n+1}) \in N$. Since N is free of rank N, then $rr_1y_1 + rr_2y_2 + \cdots + rr_{n+1}y_{n+1} = a_1x_1 + a_2x_2 + \cdots + a_nx_n$ for $x_1, x_2, \ldots, x_n$ a basis for N and $a_i \in R$. M and N are submodules of those over the field of fractions of R over the same Abelian group. In these vector spaces, one of which is naturally a subspace of the other, we can divide the equation we left off with by r, getting $r_1y_1 + r_2y_2 + \cdots + r_{n+1}y_{n+1} = \frac{a_1}{r}x_1 + \frac{a_2}{r}x_2 + \cdots + \frac{a_n}{r}x_n$, showing that the left linear combination is an element of the subspace. Since it's a list of more than n vectors, the terms of the sum are linearly dependent in the n-dimensional vector space. The coefficients giving this linear dependence can be each multiplied by the product of all their denominators to yield an R-linear dependence. Therefore, the terms of the sum and so also y_i are linearly dependent in M. □