# 7210 HW 11

Duncan Wilkie

22 November 2022

**Problem 1** (D&F 12.1.4)**.** *Let $R$ be an integral domain, let $M$ be an $R$-module, and let $N$ be a submodule of $M$. Suppose $M$ has rank $n$, $N$ has rank $r$, and the quotient $M/N$ has rank $s$. Prove that $n = r + s$.*

*Proof.* Let $x_1, x_2, \ldots, x_s$ be representatives of the maximal set of linearly independent cosets in $M/N$, and let $x_{s+1}, x_{s+2}, \ldots, x_{s+r}$ be a maximal set of linearly independent elements in $N$. We show that $x_1, x_2, \ldots, x_s, x_{s+1}, x_{s+2}, \ldots, x_{s+r}$ is a maximal set of linearly independent elements in $M$. Linear independence in $M/N$ means no nonzero linear combination of representatives of the cosets can ever be in $N$; since, by the submodule axioms, all linear combinations of $x_{s+1}, x_{s+2}, \ldots, x_{s+r}$ must be in $N$, this means that $a_1x_1 + a_2x_2 + \cdots + a_sx_s + a_{s+1}x_{s+1} + \cdots + a_{s+r}x_{s+r}$ is of the form $m + n$ for some nonzero $m \in M$, $n \in N$. If $m + n = 0 \Leftrightarrow m = -n$, then $a_1x_1 + a_2x_2 + \cdots + a_sx_s \in N$ by closure of $N$ under negation, contradicting linear independence of $x_1, x_2, \ldots, x_s$. This large list is therefore certainly linearly independent

For any nonzero $x_0 \in M$, consider the linear combination

$$a_0x_0 + a_1x_1 + \cdots + a_sx_s + a_{s+1}x_{s+1} + \cdots + a_{s+r}x_{s+r}.$$

By maximal linear independence of the cosets represented by $x_1, x_2, \ldots, x_s$, there must exist some $a_0$ (likely dependent on $a_1, a_2, \ldots, a_s$) such that $a_0x_0 + a_1x_1 + \cdots + a_sx_s \in N$. This linear combination is therefore of the form

$$n + a_{s+1}x_{s+1} + a_{s+2}x_{s+2} + \cdots + a_{s+r}x_{s+r}$$

for $n \in N$; by maximal linear independence of $x_{s+1}, x_{s+2}, \ldots, x_{s+r}$ in $N$ and the fact that linear independence is preserved under scalar multiplication in any module over an integral domain, there must exist $a', a'_{s+1}, a'_{s+2}, \ldots, a'_{s+r}$ such that

$$a'n + a'_{s+1}a_{s+1}x_{s+1} + a'_{s+2}a_{s+2} + \cdots + a'_{s+r}a_{s+r}x_{s+r} = 0$$

Expanding the definition of $n$ and distributing, one obtains an $R$-linear combination of $x_0, x_1, \ldots, x_s, x_{s+1}, \ldots, x_{s+r}$ that evaluates to zero, so the linearly independent set above is maximal. This proves $n = r + s$. $\square$

**Problem 2** (D&F 12.1.6)**.** *Show that if $R$ is an integral domain and $M$ is any non-principal ideal of $R$ then $M$ is torsion-free of rank 1 but is not a free $R$-module.*

*Proof.* $M$ is torsion-free since $R$ is an integral domain: $rm = 0$ for nonzero $r, m$ can't hold by definition. Accordingly, $M$ has rank at least 1, since any nonzero element is linearly independent.

For any two elements $n, m \in M$, one can take the $R$-linear combination $nm + (-m)n = 0$ to show that the rank is precisely 1.

If $M$ were free, then any element would be able to be uniquely written as a linear combination of basis elements, i.e. for all $m \in M$, $m = rm_0$ uniquely for unique $r \in R$ varying alongside $m$ and fixed $m_0 \in M$. However, this would mean that $M$ is a principal ideal, as every element would be a multiple of $m_0$, so $M$ can't be free. □

**Problem 3** (D&F 12.1.11). *Let $R$ be a P.I.D., let $a$ be a nonzero element of $R$ and let $M = R/(a)$. For any prime $p$ of $R$ prove that*

$$p^{k-1}M/p^kM \cong \begin{cases} R/(p) & \text{if } k \leq n \\ 0 & \text{if } k > n, \end{cases}$$

*where $n$ is the power of $p$ dividing $a$ in $R$.*

*Proof.* This is proven via induction on $k$ with the isomorphism theorems. $p^kM = p^k(R/(a))$ has elements of the form $p^kr + (a)$; the left term is precisely the form of elements of $(p^k)$, so the submodule is of the form $[(p^k) + (a)]/(a)$. The numerator ideal is generated by the greatest common divisor of $p^k$ and $a$, which, if $p^k \mid a$ (i.e. $k \leq n$), is $p^k$, and otherwise is $p^n$. Therefore, $p^kM = (p^k)/(a)$ if $k \leq n$ and $p^kM = (p^n)/(a)$ otherwise. Analogously, $p^{k-1}M = (p^{k-1})/(a)$ if $k-1 < k \leq n$ and $p^{k-1}M = (p^n)/a$ otherwise. The factor module is then $[(p^{k-1})/(a)]/[(p^k)/(a)] \cong (p^{k-1})/(p^k) \cong (1)/(p) \cong R/(p)$ if $k \leq n$ by the third isomorphism theorem. If $k - 1 = n$, so $k > n$, the factor module is $[(p^{k-1})/(a)]/[(p^n)/(a)] \cong (p^{k-1})/(p^n) \cong (1)/(1) \cong 0$ If $k > n$, then the factor module is $[(p^n)/(a)]/[(p^n)/(a)] \cong (1)/(1) \cong 0$. □

**Problem 4** (D&F 12.3.19). *Prove that all $n \times n$ matrices with characteristic polynomial $f(x)$ are similar iff $f(x)$ has no repeated factors in its unique factorization over $F[x]$.*

*Proof.* Two matrices are similar iff they have the same rational canonical form. If $f(x)$ has repeated irreducible factors, say $f(x) = p_1^{\epsilon_1}p_2^{\epsilon_2}\cdots p_m^{\epsilon_m}$ where some $\epsilon_i > 1$, then the matrices whose rational canonical forms are constructed from the invariant factors

$$p_i \mid p_1^{\epsilon_1}p_2^{\epsilon_2}\cdots p_i^{\epsilon_i - 1}\cdots p_m^{\epsilon_m}$$

and

$$p_1^{\epsilon_1}p_2^{\epsilon_2}\cdots p_i^{\epsilon_i}\cdots p_m^{\epsilon_m}$$

are not similar, despite having the same characteristic polynomials.

If $f(x)$ has no repeated factors, then it must be only one irreducible factor: since each invariant factor must divide the next, and they are multiplied to yield $f(x)$, one has $a_i = ka_{i-1}$ so the product includes $a_{i-1}(ka_{i-1})$ which is a repeated factor of at least whatever irreducibles are inside $a_{i-1}$. Accordingly, if $f(x)$ has no repeated factors, the only possible rational canonical form is that with the single, irreducible invariant factor. Such matrices are then necessarily similar. □

**Problem 5** (D&F 12.3.21). *Show that if $A^2 = A$ then $A$ is similar to a diagonal matrix which has only 0's and 1's along the diagonal.*

*Proof.* If $A = 0$, we're done; the matrix is diagonalized. Similarly if $A = I$. Therefore, since $A^2 = A$ implies $m_T(A) \mid x^2 - x = x(x-1)$, the minimal polynomial of $A$ is $x^2 - x$. This has no repeat factors, so the Jordan canonical form of $A$ is diagonal. Since this diagonal form also satisfies the same minimal polynomial, $\lambda(\lambda - 1) = 0$ for all diagonal entries, i.e. all diagonal entries are either 0 or 1. □