Abstract Algebra II Homework 7

Carson Connard

Section 12.1

1 Let M be a module of the integral domain R.

(a) Suppose x is a nonzero torsion element in M. Show that x and 0 are "linearly dependent." Conclude that the rank of $\text{Tor}(M)$ is 0, so that in particular any torsion R-module has rank 0.

Proof. By definition, $rx = 0$ for $r \neq 0$. Therefore, there do not exist any linearly independent sets as this only gives the trivial case. □

(b) Show that the rank of M is the same as the rank of the (torsion free) quotient $M/\text{Tor}(M)$.

Proof. Let us consider the subset $S + \text{Tor}(M) = \{s + \text{Tor}(M) : s \in S\} \subset M/\text{Tor}(M)$, where S is a linearly independent set of maximal order. We claim that $S + \text{Tor}(M)$ is linearly independent. Suppose that any linear combination $\sum r_i m_i$. Then for some nonzero $a \in R$, we would have that $\sum a r_i m_i = 0$, but since R is taken to be an integral domain, we have that we must have $r_i = 0$ for all i. Therefore $S + \text{Tor}(M)$ is linearly independent.

We now claim that $|S| = |S + \text{Tor}(M)|$. Suppose $a \in R$, then $am_i - am_j = 0$. Since m_i and m_j are linearly independent, we must have $a = 0$. Therefore the cardinality is the same. This gives that the rank of $M/\text{Tor}(M)$ is less than or equal to that of M. To show that it is greater than or equal to, forcing equality, take $S = \{m_i\}$ and let $S + \text{Tor}(M)$ be linearly independent. We want to show that S is linearly independent. Indeed, assume that $\sum r_i m_i = 0$. So, $\sum r_i \bar{m}_i = 0$ in $M/\text{Tor}(M)$, giving that $r_i = 0$ for all i. This gives that $S \subset M$ and S must be linearly independent. This gives that the cardinality of S is less than or equal to that of $S + \text{Tor}(M)$, implying that the rank of M is less than or equal to that of $M/\text{Tor}(M)$. So, $\text{rk}(M) = \text{rk}(M/\text{Tor}(M))$. □

2 Let M be a module of the integral domain R.

(a) Suppose that M has rank n and tha $x_1, x_2, ..., x_n$ is any maximal set of linearly independent elements of M. Let $N = Rx_1 + \cdots + Rx_n$ be the submodule generated by $x_1, ..., x_n$. Prove that N is isomorphic to R^n and that the quotient M/N is a torsion R-module.

Proof. Certainly, the R-module homomorphism $\pi_i : R^n \to N$ projecting the ith basis vector of R^n to x_i is surjective, and injectivity follows from the linear independence of the x_i's. Therefore $N \cong R^n$. Since $\text{rk}(M) = n$, we have that for any $m \in M$, the set $\{m, x_1, \cdots, x_n\}$ must be linearly dependent, and so some scalar multiple of m is the submodule N, and this is equivalent to M/N being torsion. □

(b) 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. We claim that $\text{rk}(M) = k \geq n$ (which is vacuously true), and we aim to show that $k \leq n$ to force equality. If $\{x_1, \cdots, x_k\}$ is a maximal, linearly independent set, then for any $r_1, \cdots, r_k \in R \backslash \{0\}$, the set $\{r_1 x_1, \cdots, r_k x_k\}$ must also be linearly independent. Since M/N is torsion, let us pick some $r_i \in R \setminus \{0\}$ such that $r_i x_i \in N$. Since $\text{rk}(N) = n$, along with the linear independence of the set $\{r_1 x_1, \cdots, r_k x_k\}$ gives that $k \leq n$ as desired. □

3 Let R be an integral domain and let A and B be R-modules of ranks m and n respectively. Prove that the rank of $A \oplus B$ is $m + n$.

Proof. From problem 12.1.2, we know that if R is an integral domain, M is an R-module of rank m, then there exists a submodule of M of rank m, giving that M/N is torsion. So, we can say that there exist free submodules $A_1 \subset A$ and $B_1 \subset B$ of ranks n and m such that A/A_1 and B/B_1 are torsion. Notice that certainly $A \oplus B_1 \subset A \oplus B$ is free. Since the categorical product of quotient R-modules is isomorphic to the quotient of categorical products of R-modules, we have that $(A \oplus B)/(A_1 \oplus B_1) \cong (A/A_1) \oplus (B/B_1)$. This gives then that $(A \oplus B)/(A_1 \oplus B_1)$ is torsion. Using again 12.1.2, we have that since the rank of $A_1 \oplus B_1$ is $m + n$, then so must $A \oplus B$. □

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. Suppose that $x_1, ..., x_s \in M$ are a set of elements such that the images are a maximal, linearly independent set in M/N. Take $x_{s+1}, ..., x_{s+r}$ to be a set of linearly independent elements of N. Suppose now that there exist elements $a_1, ..., a_{r+s} \in R$ such that $\sum_{i=1}^{r+s} a_i x_i = 0$. If we rearrange the expansion, we have that

$$a_1 x_1 + \cdots + a_s x_s = -(a_{s+1} x_{s+1} + \cdots + a_{r+s} x_{r+s}) \in N.$$

So, we have that $a_1 x_1 + \cdots + a_s x_s \equiv 0 \bmod N$, giving that $a_i = 0$ for $1 \le i \le s$. So, we have that $a_{s+1} x_{s+1} + \cdots + a_{r+s} x_{r+s} = 0$, giving that $a_j = 0$ for $s + 1 \le j \le r + s$. So, we have that the x_i are all linearly independent, for $1 \le i \le r + s$.

Take now some element $y \in M$. If $y \in N$ then the set $\{y, x_{s+1}, \cdots , x_{r+s}\}$ is not linearly independent. That is, there exists some k such that $ky = k_{s+1} x_{s+1} + \cdots + k_{r+s} x_{r+s}$ for $k_i \in R$. If y isn't necessarily in N, then we have that the set $\{y, x_1, \cdots , x_s\}$ is not linearly independent modulo N, and so there must exist $a_0, a_1, \cdots , a_s$ such that $a_0 y \equiv a_1 x_1 + \cdots + a_n x_n \bmod N$. The difference of these two is an element of N, so some multiple of the difference can be written as a linear combination of $x_{s+1}, \cdots , x_{r+s}$ by the above, and so there is some $r \in R$ such that $ry \in \text{span}(x_1, ..., x_{r+s})$.

Applying problem 12.1.2 yields the desired result. □

5 Let $R = \mathbb{Z}[x]$ and let $M = (2, x)$ be the ideal generated by 2 and x, considered as a submodule of R. Show that $\{2, x\}$ is not a basis of M.

Proof. Notice that the set is not $\mathbb{Z}[x]$-linearly independent. Indeed, $(-x) \cdot 2 + 2 \cdot x = 0$ is a nontrivial dependence. □

9 Give an example of an integral domain R and a nonzero torsion R-module M such that $\text{Ann}(M) = 0$. Prove that if N is a finitely generated torsion R-module then $\text{Ann}(N) \neq 0$.

Example: Consider the $\mathbb{Z}$-module $M = \bigoplus_{k \in \mathbb{N}} \mathbb{Z}/(2^k)$. Each element $m \in M$ is annihilated by 2^ℓ, where ℓ is the largest nonzero component of m. Indeed, we can write $m = (m_1 + \mathbb{Z}/(2^1), m_2 + \mathbb{Z}/(2^2), ..., a_k + \mathbb{Z}/(2^k), ...)$, so that $2^k m = 0$, giving that it is a torsion $\mathbb{Z}$-module. We claim that any element of $\text{Ann}(M)$ is in fact $0 \in \mathbb{Z}$. Take $r \in \text{Ann}(M)$, and take k such that $r < 2^k$. Consider $m = (0, 0, ..., 1 + \mathbb{Z}/(2^k), 0, ...) \in M$. The only nonzero entry is in the kth place, and since $r \in \text{Ann}(M)$, we have that $0 = ra = m$. This must give that $r = 0$ though, since $r < 2^k$. Therefore $\text{Ann}(M) = 0$.

Proof. Recall that since N is finitely generated, there exists some finite set $A \subset N$ such that $N = RA$. Since N is torsion, we have that for each $a_i \in A$ there exists some $r_i \in R$ such that $r_i a_i = 0$. Define $r = \prod_i r_i \in R$. Notice that $r \neq 0$ since $r_i \neq 0$ for all i and R is taken to be an integral domain. We will show that $r \in \text{Ann}(M)$, that is $rn = 0$ for $n \in N$, which gives that $\text{Ann}(M) \neq 0$.

Take $n \in N$, and finite generation gives that $n = s_1 a_1 + s_2 a_2 + \cdots + s_n a_n$ for $s_i \in R$. Since R is an integral domain, it is commutative, so we can change the order of multiplication in $\prod_i r_i$. So, for each i we can write $r = \hat{r}_i r_i$, where $\hat{r}_i = \prod_{j \neq i} r_j$. Then $ra_i = \hat{r}_i r_i a_i = \hat{r}_i \cdot 0 = 0$ for each i. Therefore, we have that

$$rn = r(s_1 a_1 + s_2 a_2 + \cdots + s_n a_n) = rs_1 a_1 + rs_2 a_2 + \cdots + rs_n a_n = s_1 ra_1 + s_2 ra_2 + \cdots + s_n ra_n = 0.$$

□

10 For p a prime in the PID R and N an R-module prove that the p-primary component of N is a submodule of N and prove that N is the direct sum of its p-primary components (there need not be finitely many of them).

Proof. Suppose that x, y are annhilated by a power of p, and consider p^α to be the maximum power such that both x, y are annhilated by it. So, for any $r \in R$, we have that $p^\alpha(x+ry) = p^\alpha x + rp^\alpha y = 0$. Therefore, the p-primary component of N is a submodule by the submodule criterion.

Next, suppose that $x \in N$. By unique factorization, we can write $\operatorname{Ann}(x) = up_1^{\alpha_1} \cdots p_n^{\alpha_n}$. Theorem 7 gives that $x \in \bigoplus_{i=1}^n N_{p_i} \subset \sum_p N_p$. Therefore $N = \sum_p N_p$ and it suffices to show that the sum is direct. So, suppose that nonzero $x \in N_p \cap (N_{p_1} + \cdots + N_{p_r})$ for some set of primes p, p_i. We write $x = x_1 + \cdots + x_r$, where each $x_i \in N_{p_i}$. Then there exists some α_i such that $p_i^{\alpha_i} x_i = 0$ for each i. Take $n = \prod_{i=1}^r p_i^{\alpha_i}$, giving $nx = 0$. This implies that $p|n$, and unique factorization gives that p must in fact be one of the p_i. Therefore, the sum is direct. □

11 Let R be a PID, let $a \in R$ be nonzero, and let $M = R/(a)$. For any prime $p \in R$ prove that

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

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

Proof. Let $I = (p^{k-1}, a)$ and $J = (p^k, a)$ be ideals of R. Consider the restriction of the map $R \to R/(a) = M$ to I, which we can write as the R-module homomorphism $\phi : I \to p^{k-1}M$. The isomorphism theorems give that $I/J \cong p^{k-1}M/p^kM$ as R-modules. If we take $\alpha = \gcd\{p^{k-1}, a\}$ and $\beta = \gcd\{p^k, a\}$, then we have that $I = \alpha R$ and $J = \beta R$. The isomorphism theorems applied to the projection (surjection) $R \to \alpha R$ defined by $1 \mapsto \alpha$, we have that $I/J = R/(\beta/\alpha)$. Finally, $\beta/\alpha = p$ if $k \leq n$, and is 1 if $k > n$ as desired. □

12 Let R be a PID and let $p \in R$ be a prime. Incomplete

(a) Let M be a finitely generated torsion R-module. Use the previous exercise to prove that $p^{k-1}M/p^kM \cong F^{n_k}$ where F is the field $R/(p)$ and n_k is the number of elementary divisors of M which are powers p^α with $\alpha \geq k$.

(b) Suppose M_1 and M_2 are isomorphic finitely generated torsion R-modules. Use (a) to prove that, for every $k \geq 0$, M_1 and M_2 have the same number of elementary divisors p^α with $\alpha \geq k$. Prove that this implies M_1 and M_2 have the same set of elementary divisors.

14 Let R be a PID and let M be a torsion R-module. Prove that M is irreducible if and only if $M = Rm$ for any nonzero $m \in M$ where the annihilator of m is a nonzero prime ideal (p).

Proof. ($\Longrightarrow$) Certainly, M is generated by m, as otherwise there would exist a nontrivial submodule. Assume that $\operatorname{Ann}(m) = (r)$ for a non-prime and nonzero r. That is, we write $r = ab$ for $a, b \neq 0_R, 1_R$. We aim to show that $Rbm \subset Rm = M$. Suppose not, then we can write $cbm = m$ for $c \in R$, and so $acbm = am$ therefore $am = 0$. But since $(r) \subset (a)$, this is a contradiction.

($\Longleftarrow$) Take nonzero $rm \in M$. Therefore we have that $p \nmid r$, and there exist $a, b \in R$ such that $ar + bp = 1$. We have then $arm = (ar + bp)m = m$, and so $Rrm = M$, and M has no trivial submodules as desired. □

20 Let R be an integral domain with quotient field F and let M be any R-module. Prove that the rank of M equals the dimension of the vector space $F \otimes_R M$ over F.

Proof. Assume that $\ker(\phi : M \to F \otimes_R M) = \operatorname{Tor}(M)$. First, we show that we can express each element of $F \otimes_R M$ as a multiple (over F) of a simple tensor in $\operatorname{im}\phi$. Indeed, we have that a simple tensor of $F \otimes_R M$ are of the form $(a/b) \otimes m$, so we either have that $a/b = 0$ and therefore we can rewrite as $0(1 \otimes m)$, or we have that if $a/b \neq 0$ that we can rewrite as $(a/b)(1 \otimes m)$. The set of multiples over F of elements in imϕ is closed under addition, that is

$$\begin{aligned}\frac{a_1}{b_1}(1 \otimes m_1) + \frac{a_2}{b_2}(1 \otimes m_2) &= \frac{1}{b_1 b_2}(b_2 a_1(1 \otimes m_1) + b_1 a_2(1 \otimes m_2)) \\ &= \frac{1}{b_1 b_2}(1 \otimes (b_2 a_1 m_1 + b_1 a_2 m_2)),\end{aligned}$$

and so we can express any element of $F \otimes_R M$ as a linear combination of elements of imϕ.

Consider now a linearly independent set in $F \otimes_R M$, which we write as $\{f_i(1 \otimes m_i)\}$. We have then that trivially, $\{1 \otimes m_i\}$ is a linearly independent set within $F \otimes RM$. We claim now that $\{m_i\}$ is linearly independent over R in M. So, assume that $r_i \in R$, with finitely many nonzero, such that $\sum r_i m_i = 0$. Equivalently, $\sum r_i(1 \otimes m_i) = 0$. Since we know that $\{1 \otimes m_i\}$ is linearly independent, we have that $r_i = 0$ for all i. Therefore we have that $\{m_i\}$ must indeed be linearly independent over R.

Now, let $\{m_i\}$ be a linearly independent subset of M over R. We want to show that $\{1 \otimes m_i\}$ is a linearly independent subset of $F \otimes RM$ over F. So, assume that there exist $f_i \in F$, with finitely many nonzero, such that $\sum f_i(1 \otimes m_i) = 0$. Notice that the f_i could be fractions, so let us multiply all the f_i by, say, the least common multiple of all the denominators. This allows us to rewrite as $\sum r_i(1 \otimes m_i) = 0$, where the r_i are simply multiples of the f_i. This gives that $1 \otimes \sum r_i m_i = 0$, and since $\ker \phi = \text{Tor}(M)$, there is some nonzero $r \in R$ such that $\sum r r_i m_i = 0$. By linear independence over R, we must have that $r r_i = 0$ for each i, however since $r \neq 0$ by assumption, we have that $r_i = 0$ for all i. Therefore, each f_i is a zero divisor and therefore equal to 0. So, $\{1 \otimes m_i\}$ is a linearly independent set.

So, since we found an F linearly independent subset of $F \otimes_R M$ with the same cardinality as an R linearly independent subset of M (and the converse), we have that $\text{rk}_R(M) = \dim_F(F \otimes_R M)$. □

21 Prove that a finitely generated module over a PID is projective if and only if it is free.

Proof. ($\Longleftarrow$) Recall first from a lecture from a while ago that a module is projective if it is free (or more generally, is a direct summand of a free module).

($\Longrightarrow$) Again notice that a projective module is a direct summand of a free module. Also, note that a free module of an integral domain is necessarily torsion-free. The fundamental theorem of finitely generated modules over a PID gives then that a torsion free, finitely generated module over a PID is free. □

22 Let R be a PID that is not a field. Prove that no finitely generated R-module is injective.

Proof. Consider some finitely generated R-module M. By definition, there exists some set $\{m_1, ..., m_n\}$ which generates M. Also, recall that a module M is injective if and only if for some submodule N of a module P and any homomorphism $f : N \to M$, there exists an extension $\tilde{f} : P \to M$ such that $\tilde{f}|_N = f$. We show that M is not injective.

Since R is a PID, there exists a nonzero nonunit element, say a. Consider the ideal $(a) \subset R$ as a submodule, and define the homomorphism $f : (a) \to M$ as $f(ar) = am_r$, where $ar \in (a)$ and $am_r \in M$. Suppose for the sake of contradiction that M is injective. Then there exists some extension $\tilde{f} : R \to M$ (where R is considered as an R-module) such that $\tilde{f}|_{(a)} = f$. Consider the image of 1 under $\tilde{f}$. We see that $\tilde{f}(1) = m \in M$, and since $\tilde{f}$ is an extension, we have that $\tilde{f}(a) = f(a) = am$. Now since $a \neq 0_R, 1_R$, there exists some noninvertible $b \in R$ such that $ab \neq 0$ and $a \neq b$. We have that $\tilde{f}(b) = bm' \in M$, with $m' \in M$. Since $\tilde{f}$ is a homomorphism, we have that $\tilde{f}(ab) = \tilde{f}(a)\tilde{f}(b)$. Substituting, we see $am_{bm'} = \tilde{f}(ab) = \tilde{f}(1) = m$. Therefore $am_{bm'} = m$, and so $am = m(1 - bm')$, giving that m is a multiple of am in M. However, since m is a generator, we have that it cannot be a multiple of am unless $a = 1_R$, which we assumed it is not. Therefore we have a contradiction, and M is not injective. □

Section 12.2

1 Prove that similar linear transformations of V (or $n \times n$ matrices) have the same characteristic and the same minimal polynomial.

Proof. Note first that if two matrices are similar, then they have the same canonical form, and so they have the same invariant factors. By definition, the largest invariant factor is the minimal polynomial, and the product of the invariant factors is the characteristic polynomial. Certainly then, they are the same. □

8 Verify that $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is the characteristic polynomial of the companion matrix

$$A = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{bmatrix}.$$

Proof. We proceed via induction on n. As a base case, if $n = 1$, then trivially $\det(xI - A) = x + a_0$. Assume then that

$$\det \begin{bmatrix} x & 0 & 0 & \cdots & 0 & a_0 \\ -1 & x & 0 & \cdots & 0 & a_1 \\ 0 & -1 & x & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \\ 0 & 0 & 0 & \cdots & -1 & x + a_{n-2} \end{bmatrix} = x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0.$$

Expanding along the first row gives us

$$\begin{aligned} \det(xI - A) &= \det \begin{bmatrix} x & 0 & 0 & \cdots & 0 & a_0 \\ -1 & x & 0 & \cdots & 0 & a_1 \\ 0 & -1 & x & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \\ 0 & 0 & 0 & \cdots & -1 & x + a_{n-1} \end{bmatrix} \\ &= x(x^{n-1} + a_{n-1}x^{n-1} + \cdots + a_2 x + a_1) + (-1)^{n+1} a_0 \det \begin{bmatrix} -1 & x & & \\ & \vdots & \vdots & \\ & & -1 & x \end{bmatrix} \\ &= x^n + a_{n-1}x^{n-1} + \cdots + a_2 x^2 + a_1 x + (-1)^{n+1} a_0 (-1)^{n-1} \\ &= x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0. \end{aligned}$$

We have shown the desired result. □

10 Find all similarity classes of 6 × 6 matrices over $\mathbb{Q}$ with minimal polynomial $(x + 2)^2(x - 1)$.

Solution. We know that the minimal polynomial is the largest invariant factor. Also, the product of the invariant factors must be a degree 6 polynomial. So, we have the following possible characteristic polynomials: $(x+2)^5(x-1)$, $(x+2)^4(x-1)^2$, $(x+2)^3(x-1)^3$, $(x+2)^2(x-1)^4$. Then we can derive invariant factors, and give an example of a matrix for each:

1. $x - 1$, $x - 1$, $x - 1$, $(x + 2)^2(x - 1)$,

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -3 \end{bmatrix}$$

2. $x+2$, $x+@$, $x+2$, $(x+2)^2(x-1)$,

$$\begin{bmatrix} -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -3 \end{bmatrix}$$

3. $x+2$, $(x+2)^2$, $(x+2)^2(x-1)$,

$$\begin{bmatrix} -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -4 & 0 & 0 & 0 \\ 0 & 1 & -4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -3 \end{bmatrix}$$

4. $x-1$, $(x+2)(x-1)$, $(x+2)^2(x-1)$,

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -3 \end{bmatrix}$$

5. $x+2$, $(x+2)(x-1)$, $(x+2)^2(x-1)$,

$$\begin{bmatrix} -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -3 \end{bmatrix}$$

6. $(x+2)^2(x-1)$, $(x+2)^2(x-1)$,

$$\begin{bmatrix} 0 & 0 & 4 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -3 \end{bmatrix}$$

20 Let ℓ be a prime and let $\Phi_\ell(x) = (x^\ell - 1)/(x-1) = x^{\ell-1} + x^{\ell-2} + \cdots + x + 1 \in \mathbb{Z}[x]$ be the ℓth cyclotomic polynomial, which is irreducible over $\mathbb{Q}$. Incomplete

(a) Show that if $p = \ell$ then $\Phi_\ell(x)$ is divisible by $x-1$ in $\mathbb{F}_\ell[x]$.

(b) Suppose $p \neq \ell$ and let f denote the order of p in $\mathbb{F}_\ell^\times$, i.e., f is the smallest power of p with $p^f \equiv 1 \bmod \ell$. Show that $m = f$ is the first value of m for which the group $GL_m(\mathbb{F}_p)$ contains an element A of order ℓ.

(c) Show that $\Phi_\ell(x)$ is not divisible by any polynomial of degree smaller than f in $\mathbb{F}_p[x]$. Let $m_A(x) \in \mathbb{F}_p[x]$ denote the minimal polynomial for the matrix A in (b) and conclude that $m_A(x)$ is irreducible of degree f and divides $\Phi_\ell(x)$ in $\mathbb{F}_p[x]/$

(d) In particular, prove that $\Phi_\ell(x)$ is irreducible modulo p if and only if $\ell - 1$ is the smallest power of p which is congruent to 1 modulo ℓ, i.e. p is a primitive root modulo ℓ.