Abstract Algebra II Homework 8

Carson Connard

Section 12.3

1 Suppose the vector space V is the direct sum of cyclic $F[x]$-modules whose annihilators are $(x+1)^2$, $(x-1)(x^2+1)^2$, (x^4-1), and $(x+1)(x^2-1)$. Determine the invariant factors and elementary divisors for V.

Solution. We can decompose V as follows:

$$\begin{aligned} V = \big(F[x]/(x^2+1)\big) \oplus \big(F[x]/(x-1) \oplus F[x]/(x^2+1)^2\big) \\ \oplus \big(F[x]/(x^2+1) \oplus F[x]/(x-1) \oplus F[x]/(x+1)\big) \\ \oplus \big(F[x]/(x+1)^2 \oplus F[x]/(x-1)\big). \end{aligned}$$

We have then that the elementary divisors are $(x+1)^2$, $(x+1)^2$, $(x+1)$, $(x-1)$, $(x-1)$, $(x-1)$, $(x^2+1)^2$, and (x^2+1). We can combine these like we grouped the decomposition before to give invariant factors $(x+1)^2(x-1)(x^2+1)^2$, $(x+1)^2(x-1)(x^2+1)$, and $(x+1)(x-1)$.

18 Determine all possible Jordan canonical forms for a linear transformation with characteristic polynomial $(x-2)^3(x-3)^2$.

Solution. Observe that the characteristic polynomial has eigenvalues 2 and 3, with multiplicities 3 and 2 respectively. Let $J_i(\lambda)$ denote a Jordan block with respect to the eigenvalue λ, with multiplicity i. Then the Jordan canonical form is as follows:

1. $J_1 \cong J_3(2) \oplus J_2(3)$
2. $J_2 \cong J_1(2) \oplus J_2(2) \oplus J_2(3)$
3. $J_3 \cong J_1(2) \oplus J_1(2) \oplus J_1(2) \oplus J_2(3)$
4. $J_4 \cong J_3(2) \oplus J_1(3) \oplus J_1(3)$
5. $J_5 \cong J_1(2) \oplus J_2(2) \oplus J_1(3) \oplus J_1(3)$
6. $J_6 \cong J_1(2) \oplus J_1(2) \oplus J_1(2) \oplus J_1(3) \oplus J_1(3)$.

So, we have

$$J_1 = \begin{bmatrix} 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix}, \quad J_2 = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix}, \quad J_3 = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix}$$

$$J_4 = \begin{bmatrix} 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix}, \quad J_5 = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix}, \quad J_6 = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 3 \end{bmatrix}$$

19 Prove that all $n \times n$ matrices with characteristic polynomial $f(x)$ are similar if and only if $f(x)$ has no repeated factors in its unique factorization in $F[x]$.

Proof. ($\Longrightarrow$) Suppose first that f does indeed have a repeated factor in its unique factorization in $F[x]$. That is, without loss of generality, $f = f_1 \cdot f_2 \cdots f_k$, but $f_1 = f_2$, with each $f_i \in F[x]$ being of degree at least 1. Without loss of generality, we can take all f_i and f itself to be monic. Set $g = f_1$ and $h = f_3 \cdots f_k$ now, so $f = g^2 h$. If we consider the matrices

$$A = C_f, \quad B = \begin{bmatrix} C_g & 0 \\ 0 & C_{g \cdot h} \end{bmatrix},$$

where C_ϕ denotes the companion matrix of the polynomial ϕ. Since g divides gh, both matrices are in rational canonical form, and have characteristic polynomial $f = g \cdot g \cdot h$. But, since their rational canonical forms are different, they are not similar.

($\Longleftarrow$) Suppose that $f(x)$ has no repeated factors in its unique factorization. We know C_f has characteristic polynomial f. Suppose that A is some matrix which also has characteristic polynomial f, and let $a_1(x), ..., a_m(x) \in F[x]$ denote A's invariant factors. Note that the characteristic polynomial of f is trivially $f = a_1 \cdots a_m$. If $m > 1$, then $a_1 \mid a_2$. If f_1 is an irreducible factor of a_1 in $F[x]$, then $f_1^2 \mid f$, meaning that f has a repeated factor in its unique factorization, giving a contradiction. So, $m = 1$ and $a_1 = f$. □

31 Let N be an $n \times n$ matrix with coefficients in the field F. The matrix N is said to be nilpotent if some power of N is the zero matrix, that is $N^k = 0$ for some k. Prove that any nilpotent matrix is similar to a block diagonal matrix whose blocks are matrices with 1's along the first superdiagonal and 0 elsewhere.

Proof. Let $u \neq 0$ be such that $N^{k-1}u \neq 0$. Observe that $\{u, Nu, ..., N^{k-1}u\}$ is linearly independent. So for $a_0, a_1, ..., a_{k-1} \in F$, it is clear that $a_0 u + a_1(Nu) + \cdots + a_{k-1}(N^{k-1}u) = 0$ has only the trivial solution. Consider the following two cases:

Case 1: $k \geq n$. The matrix representation for N with respect to the basis $\{N^{n-1}u, ..., Nu, u\}$ is given as

$$\begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix},$$

which consists of a single Jordan block whose entries are 1 along the superdiagonal and 0 elsewhere.

Case 2: $k < n$. Since there is a unique pair of integers q, r such that $n = qk + r$, with $0 \leq r \leq k - 1$, consider a $k \times k$ submatrix, Q, contained in N. Then its representation for K with respect to a basis $\{u, Nu, ..., N^{k-1}u\}$ is given as

$$\begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Now take R to be an $r \times r$ matrix. Then the representation matrix for R with respect to the basis $\{N^{k-1}u, ..., N^{k-r-1}u, N^{k-r}u\}$ is given as

$$\begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \ddots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{bmatrix},$$

and therefore $N \cong Q \oplus \cdots \oplus Q \oplus R$, where $Q \oplus \cdots \oplus Q$ is q copies of a $k \times k$ submatrix Q. Therefore, N is similar to a block diagonal matrix whose entries are 1 on the superdiagonal and 0 elsewhere.

□

34 Prove that the trace of a nilpotent $n \times n$ matrix is 0.

Proof. Let M be such a matrix. Since a nilpotent matrix N is similar to M, we have that M and N have the same characteristic polynomial, namely $p(x) = \det(xI - N) = \det(xI - M) = x^n$. Observe the coefficient for x^{n-1}, which is equivalent to the trace of M, is equal to 0. Therefore the trace is 0. □

43 Prove that if A and B are commuting matrices then $\exp(A + B) = \exp(A)\exp(B)$.

Proof. Recall that $\exp(x) = \sum_{k\in\mathbb{N}} x^k/k!$ is a formal power series over a field of characteristic 0. Consider the ring $F[[x]][[y]]$ of formal power series of x over y. Let $p(x)$ be a polynomial, and $G(x)$ be a formal power series. Then $G(p(x))$ is the formal power series which is obtained by combining like terms. We compute the following:

$$\begin{aligned}
\exp(x+y) &= \sum_{t\in\mathbb{N}} \frac{1}{t!}(x+y)^t \\
&= \sum_{t\in\mathbb{N}} \frac{1}{t!} \sum_{k=0}^{t} C_k^t x^k y^{t-k} \\
&= \sum_{t\in\mathbb{N}} \sum_{k=0}^{t} \frac{1}{k!}\frac{1}{(t-k)!} x^k y^{t-k} \\
&= \sum_{t\in\mathbb{N}} \sum_{h+k=t} \frac{1}{k!}x^k \frac{1}{h!}y^h \\
&= \sum_{h\in\mathbb{N}} \sum_{k\in\mathbb{N}} \frac{1}{k!}x^k \frac{1}{h!}y^h \\
&= \left(\sum_{k\in\mathbb{N}} \frac{x^k}{k!}\right)\left(\sum_{h\in\mathbb{N}} \frac{y^h}{h!}\right) \\
&= \exp(x)\exp(y).
\end{aligned}$$

Indeed, if A and B are commuting matrices, then we have that this gives the desired result. □

45 Let N be the $r \times r$ matrix with 1's on the first superdiagonal and 0 elsewhere. Compute the exponential of the following nilpotent $r \times r$ matrix:

$$\text{if } Nt = \begin{bmatrix} 0 & t & & & \\ & 0 & t & & \\ & & \ddots & \ddots & \\ & & & 0 & t \\ & & & & 0 \end{bmatrix}, \text{ then } \exp(Nt) = \begin{bmatrix} 1 & t & \frac{t^2}{2!} & \cdots & \cdots & \frac{t^{r-1}}{(r-1)!} \\ & 1 & t & \frac{t^2}{2!} & & \vdots \\ & & \ddots & \ddots & \ddots & \vdots \\ & & & \vdots & t & \frac{t^2}{2!} \\ & & & & 1 & t \\ & & & & & 1 \end{bmatrix}.$$

Deduce that if J is the $r \times r$ elementary Jordan matrix with eigenvalue λ then

$$\exp(Jt) = \begin{bmatrix} e^{\lambda t} & te^{\lambda t} & \frac{t^2}{2!}e^{\lambda t} & \cdots & \cdots & \frac{t^{r-1}}{(r-1)!}e^{\lambda t} \\ & e^{\lambda t} & te^{\lambda t} & \frac{t^2}{2!}e^{\lambda t} & & \vdots \\ & & \ddots & \ddots & \ddots & \vdots \\ & & & \ddots & te^{\lambda t} & \frac{t^2}{2!}e^{\lambda t} \\ & & & & e^{\lambda t} & te^{\lambda t} \\ & & & & & e^{\lambda t} \end{bmatrix}.$$

50 Fix any $A \in M_n(K)$. Prove that the map $K \to GL_n(K)$ defined by $t \mapsto \exp(At)$ is a group homomorphism (here K is the additive group of the field).

Proof. If we assume first that $\exp(At)$ is nonsingular, and we take ϕ_A to be the map in question, then the result from exercise 43 gives the following:

$$\phi_N(r_1 + r_2) = \exp(A(r_1 + r_2)) = \exp(Ar_1 + Ar_2) = \exp(Ar_1)\exp(Ar_2) = \phi_A(r_1)\phi_A(r_2).$$

□

52 Deduce from the fact that if $G(x) = \sum_{k=0}^{\infty} \alpha_k x^k$ then $\frac{d}{dt}G(At) = A\sum_{k=1}^{\infty} k\alpha_k (At)^{k-1}$, that $\frac{d}{dt}\exp(At) = A\exp(At)$.

Proof. Consider A to be an $n \times n$ matrix with entries in $\mathbb{C}$. Define the map $t \overset{\phi}{\mapsto} \exp(At)$. The property specified allows us to write the following:

$$\begin{aligned}
\frac{d}{dt}\exp(At) &= \frac{d}{dt}\sum_k \frac{(At)^k}{k!} \\
&= A\sum_k \frac{1}{(k+1)!}(k+1)(At)^k \\
&= A\sum_k \frac{1}{k!}(At)^k \\
&= A\exp(At).
\end{aligned}$$

□

Section 13.1

1 Show that $p(x) = x^3 + 9x + 6$ is irreducible in $\mathbb{Q}[x]$. Let θ be a root of $p(x)$. Find the inverse of $1 + \theta$ in $\mathbb{Q}(\theta)$.

Proof. Consider the Eisenstein criterion. From $p(x)$, we get that the prime specified by Eisenstein's criterion is $p = 3$, such that $3 \mid 9, 6$ and $3 \nmid 1$, and $3^2 \nmid 6$. Therefore, we have that $p(x)$ is irreducible in $\mathbb{Q}[x]$.

Next, take θ to be a root of $p(x)$, that is $p(\theta) = \theta^3 + 9\theta + 6 = 0$. By the Euclidean algorithm, we have that there are polynomials $a(x), b(x) \in \mathbb{Q}[x]$ such that $a(x)(1 + x) + b(x)(x^3 + 9x + 6) = 1$. Long division gives the desired computation:

$$\begin{aligned}
x^3 + 9x + 6 &= x^3 + 9x + 10 - 4 \\
x^3 + 9x + 6 &= (1 + x)(x^2 - x + 10) - 4 \\
-(1 + x)(x^2 - x + 10) + x^3 + 9x + 6 &= -4 \\
\frac{(1 + x)(x^2 - x + 10)}{4} + \frac{x^3 + 9x + 6}{-4} &= 1 \\
\implies \frac{(1 + \theta)(\theta^2 - \theta + 10)}{4} + \frac{\theta^3 + 9\theta + 6}{-4} &= 1 \\
\frac{(1 + \theta)(\theta^2 - \theta + 10)}{4} + 0 &= 1 \\
\frac{1}{1 + \theta} &= \frac{\theta^2 - \theta + 10}{4}.
\end{aligned}$$

□

4 Prove directly that the map $\phi : a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is an isomorphism of $\mathbb{Q}(\sqrt{2})$ with itself.

Proof. First we check additive structure:

$$\begin{aligned}\phi\left((a+b\sqrt{2})+(c+d\sqrt{2})\right) &= \phi\left((a+c)+(b+d)\sqrt{2}\right)\\ &= (a+c)-(b+d)\sqrt{2}\\ &= \left(a-b\sqrt{2}\right)\left(c-d\sqrt{2}\right)\\ &= \phi(a+b\sqrt{2})+\phi(c+d\sqrt{2}).\end{aligned}$$

For multiplicative structure,

$$\begin{aligned}\phi\left((a+b\sqrt{2})(c+d\sqrt{2})\right) &= \phi((ac+2bd)+(ad+bc)\sqrt{2})\\ &= (ac+2bd)-(ad+bc)\sqrt{2}\\ &= (ac+2bd)+(-ad-bc)\sqrt{2}\\ &= \phi(a+b\sqrt{2})\phi(c+d\sqrt{2}).\end{aligned}$$

Injectivity holds because if $\phi(x) = \phi(y)$ for $x, y \in \mathbb{Q}(\sqrt{2})$, we have $\phi(x) = a - b\sqrt{2}$ and $\phi(y) = c - d\sqrt{2}$, therefore $a - b\sqrt{2} = c - d\sqrt{2}$. So, $a - c = (d - b)\sqrt{2}$, and if $b \neq d$ then we would have a rational number equal to an irrational, and so $b = d$. Therefore $a = c$, and therefore $x = y$.

Surjectivity holds as well. Indeed, if $y = a + b\sqrt{2}$, we want to show that there exists $x = c + d\sqrt{2}$ such that $\phi(x) = y$. We see $\phi(c + d\sqrt{2}) = c - d\sqrt{2}$. Set $a = c$ and $b = d$, and we have that $\phi(c + d\sqrt{2}) = a - (-b)\sqrt{2} = a + b\sqrt{2} = y$. □

Section 13.2

1 Let $\mathbb{F}$ be a finite field of characteristic p. Prove that $|\mathbb{F}| = p^n$ for some positive $n \in \mathbb{Z}$.

Proof. Let K be the prime subfield of $\mathbb{F}$. The vector space of $\mathbb{F}$ over K is of finite dimension, say n, and there exists some basis $\{a_1, a_2, ..., a_n\}$ of $\mathbb{F}$ over K. Since every element of $\mathbb{F}$ can be expressed as a unique linear combination of the a_i over K, every $a \in \mathbb{F}$ can be written as $a = \sum k_i a_i$ with $k_i \in K$. Since K has p elements, $\mathbb{F}$ must have p^n elements. □

4 Determine the degree over $\mathbb{Q}$ of $2 + \sqrt{3}$ and of $1 + \sqrt[3]{2} + \sqrt[3]{4}$.

Solution. Consider the polynomial $f(x) = (x - 2)^2 - 3$. If we expand this, we get $f(x) = x^2 - 4x + 1$. Plugging in $2 + \sqrt{3}$ gives 0. Since it is a root, the degree over $\mathbb{Q}$ is 2.

Consider the polynomial $g(x) = (x - 1)^3 - 2(x - 1)^2 - 4(x - 1)$. If we expand this, we get $g(x) = x^3 - 3x^2 + 3x - 1$. Plugging in $1 + \sqrt[3]{2} + \sqrt[3]{4}$ gives 0. Since it is a root, the degree over $\mathbb{Q}$ is 3.

7 Prove that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Conclude that $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$. Find an irreducible polynomial satisfied by $\sqrt{2} + \sqrt{3}$.

Proof. Certainly, $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ since $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Take now $x = \sqrt{2} + \sqrt{3}$. Then we have

$$\begin{aligned}x^2 &= (\sqrt{2}+\sqrt{3})^2 = (\sqrt{2})^2 + (\sqrt{3})^2 + 2\sqrt{2}\sqrt{3} = 5 + 2\sqrt{6},\\ x^3 &= (\sqrt{2}+\sqrt{3})^3 = (\sqrt{2}+\sqrt{3})(\sqrt{2}+\sqrt{3})^2 = (\sqrt{2}+\sqrt{3})(5+2\sqrt{6}) = 11\sqrt{2} + 9\sqrt{3}.\end{aligned}$$

We use this then to write

$$\begin{aligned}\sqrt{2} &= \frac{1}{2}[(11\sqrt{2}+9\sqrt{3}) - 9(\sqrt{2}+\sqrt{3})]\\ &= \frac{1}{2}[(\sqrt{2}+\sqrt{3})^3 - 9(\sqrt{2}+\sqrt{3})].\end{aligned}$$

Similarly, we have that

$$\begin{aligned}\sqrt{3} &= -\frac{1}{2}[(11\sqrt{2}+9\sqrt{3}) - 11(\sqrt{2}+\sqrt{3})] \\ &= -\frac{1}{2}[(\sqrt{2}+\sqrt{3})^3 - 11(\sqrt{2}+\sqrt{3})].\end{aligned}$$

Therefore, we have that both $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Therefore $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Therefore equality holds.

Certainly though, $\sqrt{2} \notin \mathbb{Q}(\sqrt{2})$, and so the extension $\mathbb{Q}(\sqrt{2},\sqrt{3})$ has degree 2 over $\mathbb{Q}(\sqrt{2})$. We have then that

$$\Big[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}\Big] = \Big[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})\Big]\Big[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}\Big] = 2 \cdot 2 = 4.$$

Since we showed that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$, we have the desired result.

Lastly, the irreducible polynomial must be of degree 4, as an extension generated by it would be of degree 4. We calculate

$$\begin{aligned}x = \sqrt{2}+\sqrt{3} \implies x^2 = 5+2\sqrt{6} \implies x^2-5 = 2\sqrt{6}, \\ (x^2-5)^2 = (2\sqrt{6})^2 \implies x^4 - 10x^2 + 25 = 24 \implies x^4 - 10x^2 + 1 = 0.\end{aligned}$$

The polynomial $f(x) = x^4 - 10x^2 + 1$ is the minimal polynomial, and is therefore irreducible. □

12 Suppose the degree of the extension K/F is a prime p. Show that any subfield E of K containing F is either K or F.

Proof. Let $F \subseteq E \subseteq K$ be fields with $[K:F] = p$. Then we have that $p = [K:F] = [K:E][E:F]$, and so either $[K:E] = 1$ or $[E:F] = 1$. Therefore, either $E = F$ or $E = K$. □

14 Prove that if $[F(\alpha):F]$ is odd, then $F(\alpha) = F(\alpha^2)$.

Proof. Since $\alpha^2 \in F(\alpha)$, we clearly have that $F(\alpha^2) \subset F(\alpha)$. So, we must prove that $\alpha \in F(\alpha^2)$. To do so, consider the polynomial $f(x) = x^2 - \alpha^2$ so that $p(\alpha) = 0$. Note that $\alpha \in F(\alpha^2)$ if and only if $f(x)$ is irreducible in $F(\alpha^2)$. For the sake of contradiction, suppose that $f(x)$ is irreducible in $F(\alpha^2)$, so that $[F(\alpha) : F(\alpha^2)] = 2$. Then $[F(\alpha):F] = [F(\alpha):F(\alpha^2)][F(\alpha^2):F] = 2[F(\alpha^2):F]$, but this gives a contradiction as this would give $[F(\alpha):F]$ is even. Therefore $f(x)$ is irreducible in $F(\alpha^2)$ and $\alpha \in F(\alpha^2)$. □

16 Let K/F be an algebraic extension and let R be a ring contained in K and containing F. Show that R is a subfield of K containing F.

Proof. Take some nonzero $r \in R$. Since r is algebraic in F, there exists an irreducible polynomial $f(x) = a_0 + a_1 x + \cdots + x^n \in F[x]$ such that $f(r) = 0$. Note however that since f is irreducible, we must have that $a_0 \neq 0$. Then $r^{-1} = a_0^{-1}(r^{n-1} + \cdots + a_1)$. Since $a_i \in F \subset R$ and $r \in R$, we have that $r^{-1} \in R$. This gives the desired result. □