Final Exam

D. Zack Garza

January 1, 2020

Contents

1 1

We prove a slightly stronger statement, namely:

Theorem: $\mathbb{Z}$ is initial in the category of unital rings and ring homomorphisms.

This means that if we are given any such ring R, there is exactly one map $\mathbb{Z} \to R$.

Then, given an abelian group A, we can take $R = \hom_{\text{Ab}}(A, A)$, the hom set of abelian group endomorphisms, which is itself a unital ring. This will imply that there is a unique map $\mathbb{Z} \to \hom_{\text{Ab}}(A, A)$, and since all such maps induce $\mathbb{Z}$-module structures on A, the result will follow.

Proof: Let R be arbitrary and 1_R be its multiplicative identity. We first show that there exists a ring homomorphism $\mathbb{Z} \to R$, namely

$$\begin{aligned}\phi : \mathbb{Z} &\to R \\ n &\mapsto \sum_{i=1}^{n} 1_R.\end{aligned}$$

Note that $\phi(1) = 1_R$ and $\phi(-1) = -1_R$, and it is routine to check that ϕ is a ring homomorphism.

Now toward a contradiction, suppose there were another such ring homomorphism $\psi : \mathbb{Z} \to R$. From the definition of a ring homomorphism, ψ must satisfy,

$$\begin{aligned}\psi(1) &= 1_R \\ \psi(-1) &= -1_R,\end{aligned}$$

and by $\mathbb{Z}$-linearity, we must have

$$\psi(n) = \psi(\sum_{i=1}^{n} 1) = \sum_{i=1}^{n} \psi(1) = \sum_{i=1}^{n} 1_R = \phi(n),$$

and so $\psi(x) = \phi(x)$ for every $x \in \mathbb{Z}$. But this precisely means that $\psi = \phi$ as ring homomorphisms. ■

2 2

2.1 a

Let $\phi : \mathbb{Z}^4 \to \mathbb{Z}^3$ be a linear map which in the standard basis $\mathcal{B}$ is represented by

$$T := [\phi]_{\mathcal{B}} = [f_1^t, f_2^t, f_3^t, f_4^t] = \begin{bmatrix} 1 & 2 & 0 & 3 \\ 0 & -3 & 3 & 1 \\ -1 & 1 & 1 & 5 \end{bmatrix}.$$

Then $\operatorname{im} T = \operatorname{span}_{\mathbb{Z}} \{f_1, f_2, f_3, f_4\} := N$ by construction.

We can then compute the echelon form

$$\begin{pmatrix} 1 & 1 & 1 & 5 \\ 0 & 3 & 1 & 8 \\ 0 & 0 & 4 & 9 \end{pmatrix},$$

which has pivots in columns $1, 2$, and 3, and thus

$$N = \text{span}_{\mathbb{Z}} \{f_1, f_2, f_3\}$$

2.2 b

Without loss of generality, we can consider the image of the reduced matrix

$$A' = \begin{pmatrix} -1 & 2 & 0 \\ 0 & -3 & 3 \\ 1 & 1 & 1 \end{pmatrix},$$

since $N = \text{im } A = \text{im } A'$.

When computing the characteristic polynomial, we find that $\chi_{A'}(x) = (x+3)(x+2)(x-2)$, which means that A' has distinct eigenvalues. We can thus immediately write

$$JCF(A) = \left[\begin{array}{c|c|c} 2 & 0 & 0 \\ \hline 0 & -2 & 0 \\ \hline 0 & 0 & -3 \end{array}\right].$$

From this, we can obtain the Smith normal form,

$$SNF(A') = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 12 \end{bmatrix},$$

which allows us to read off

$$\text{im } A' \cong \mathbb{Z} \oplus \mathbb{Z} \oplus 12\mathbb{Z},$$

and thus

$$\mathbb{Z}^3/N \cong \frac{\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}}{\mathbb{Z} \oplus \mathbb{Z} \oplus 12\mathbb{Z}} \cong \mathbb{Z}/12\mathbb{Z}..$$

3 3

The elementary divisors are given by:

$$\begin{array}{ccc} (x-1)^3 & (x^2+1)^4 & (x+2) \\ (x-1) & (x^2+1)^2 & \\ & (x^2+1)^2 & . \end{array}$$

The invariant factors are:

$$\begin{aligned} d_3 &= (x-1)^3(x^2+1)^4(x+2) \\ d_2 &= (x-1)(x^2+1)^2 \\ d_1 &= (x^2+1)^2. \end{aligned}$$

4 4

Lemma: $(2, x) \trianglelefteq \mathbb{Z}[x]$ is not a principal ideal.

Proof: If this ideal were generated by a single element $p(x)$, then $p \mid 2$ would force $p \in \mathbb{Z}$. But this means that the element $x \notin (p)$, a contradiction. ■

Suppose toward a contradiction that $J = (2, x) \trianglelefteq \mathbb{Z}[x]$ is a direct sum of cyclic submodules of $R := \mathbb{Z}[x]$.

Then write

$$J = M_1 \oplus M_2 \oplus \cdots \oplus M_n$$

where each $M_i = \alpha_i \mathbb{Z}[x]$ is a cyclic $\mathbb{Z}[x]$-module.

Note that by the lemma, we can not have $n = 1$, since this would mean $J = \alpha_1 \mathbb{Z}[x] = (\alpha_1)$ where we can identify cyclic submodules with principal ideals.

On the other hand, we also can't have $n \geq 2$. Since the sum is direct, this forces (for example) $M_1 \bigcap M_2 = \emptyset$.

However, take the two generating elements $\alpha_1, \alpha_2 \in \mathbb{Z}[x]$ and consider their product. Noting that $\mathbb{Z}[x]$ is a commutative ring, we have

$$\alpha_1\alpha_2 \in \alpha_1\mathbb{Z}[x] = M_1 \text{ since } \alpha_2 \in \mathbb{Z}[x] \alpha_1\alpha_2 = \alpha_2\alpha_1 \in \alpha_2\mathbb{Z}[x] = M_2 \text{ since } \alpha_1 \in \mathbb{Z}[x],$$

and so $\alpha_1\alpha_2 \in M_1 \bigcap M_2$, a contradiction. So no such direct sum decomposition is possible. ■

5 5

Irreducible: Let $a \in M$ be arbitrary; we can then consider the cyclic submodule $aR \trianglelefteq M$. Since M is irreducible, we must have $aR = 0$ or $aR = M$. If $aR = 0$ then a must be 0.

Otherwise, $aR = M$ implies that M itself is a cyclic module with generator a. Since R is a PID, we can find an element p such that $\mathrm{Ann}_R(M) = (p) \trianglelefteq R$, in which case $M \cong R/(p)$.

It is also necessarily the case that (p) is maximal, for if there were another ideal $(p) \subseteq J \trianglelefteq R$, then $J/(p) \trianglelefteq R/(p) \cong M$ is a submodule by the correspondence theorem for ideals. But this necessarily forces $J/(p) = 0$ or M by irreducibility of M, so $J = (p)$ or R.

Thus irreducible modules are exactly the cyclic modules, or equivalently those of the form $R/(p)$ where (p) is a maximal ideal.

Indecomposable: We first note that by the structure theorem for modules over a PID, any module M has a primary decomposition $M \cong \bigoplus_i R/(p_i^{k_i})$.

This means that if M is indecomposable, we must have $M \cong R/(p^n)$ (with a single summand) for some prime $p \in R$; otherwise the primary decomposition would yield additional summands. Moreover, by the Chinese Remainder Theorem, M can not be decomposed further.

Thus all indecomposable module are of the form $R/(p^n)$ for some $n \geq 1$.

6 6

Suppose $T : V \to V$ is not invertible, then $\dim \operatorname{im} T < n$ and $\dim \ker T > 0$ by the Rank-Nullity theorem. This means that there is a nontrivial $\mathbf{v} \in \ker T$, so let S be the matrix formed by the outer product $\mathbf{v}\mathbf{v}^t$.

We then consider how ST acts on vectors $\mathbf{x}$:

$$\begin{aligned}
TS\mathbf{x} &= T\mathbf{v}\mathbf{v}^t\mathbf{x} \\
&= (T\mathbf{v})\mathbf{v}^t\mathbf{x} \\
&= \mathbf{0}\mathbf{v}^t\mathbf{x} \\
&= \mathbf{0_n}\mathbf{x} \\
&= \mathbf{0},
\end{aligned}$$

where $\mathbf{0_n}$ is the $n \times n$ matrix of all zeros.

However, $\mathrm{rank}(ST) \geq 1$ since $ST = 0 \iff$ every column of T is in the nullspace of S, so ST can not be the zero matrix. ■

7 7

7.1 a

Note that if $A = 0$ or I then A is patently diagonal, so suppose otherwise. Since $A^2 = A$, we have $A^2 - A = 0$ and thus A satisfies the polynomial $p(x) = x^2 - 1 = x(x-1)$. Moreover, since $A \neq 0, I$, the minimal polynomial is at least degree – since p is monic, it must in fact be the minimal polynomial.

We can immediately deduce that the size of the largest Jordan block corresponding to $\lambda = 0$ is exactly 1, as is the size of the largest Jordan block corresponding to $\lambda = 1$. But this says that *all* Jordan blocks must be size 1, so $JNF(A)$ has no off-diagonal entries and is thus diagonal.

7.2 b

If k is the multiplicity of $\lambda = 0$ as an eigenvalue, we have

$$A \sim \left[\begin{array}{ccc|cccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right],$$

which has a $k \times k$ block of zeros and an $(n-k) \times (n-k)$ block of 1s.

8 8

In both cases, we will need the characteristic polynomials $\chi_A(x)$, since $RCF(A)$ will depend on the invariant factors of A. We will also use the fact that over the algebraic closure $\overline{\mathbb{Q}}$, the minimal and characteristic polnyomials must have the same roots.

8.1 a

Suppose $m_A(x) = (x-1)(x^2+1)^2$, which is a degree 5 polynomial. Since $\deg \chi_A$ must be 6 and m_A must divide χ_A in $\mathbb{Q}[x]$, the only possibility in this case is that

$$\chi_A(x) = (x-1)^2(x^2+2)^2.$$

To determine the possible invariant factors $\{d_i\}$, we can just note that $\prod d_i = \chi_A(x)$ and $d_n = m_A(x)$. With these constraints, the only possibility is

$$\begin{aligned} d_1 &= (x-1) \\ d_2 &= (x-1)(x^2+1)^2., \end{aligned}$$

from which we can immediately obtain the elementary divisors:

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

Then noting that

$$d_2 = d_2 = (x-1)(x^2+1)^2 = x^5 - x^4 + 4x^3 - 4x^2 + 4x - 4,$$

there is thus only one possible Rational Canonical form:

$$RCF(A) = \left[\begin{array}{c|ccccc} 1 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 1 & 0 & 0 & 0 & -4 \\ 0 & 0 & 1 & 0 & 0 & 4 \\ 0 & 0 & 0 & 1 & 0 & -4 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right].$$

8.2 b

The constraints $m_A(x) = (x^2+1)^2(x^3+1)$ with $\deg m_A(x) = 7$ and $\deg \chi_A(x) = 10$ forces

$$\chi_A(x) = (x^2+1)^2(x^3+1)^2.$$

Furthermore, the invariant factors are similarly constrained, and so the only possibility is

$$\begin{aligned} d_1 &= (x_3+1) \\ d_2 &= (x^2+1)^2(x^3+1) \end{aligned}$$

with corresponding elementary divisors

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

Noting that

$$d_2 = (x^2+1)^2(x^3+1) = x^5 + x^3 + x^2 + 1,$$

we have

$$RCF(A) = \left[\begin{array}{cc|ccccc} 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right].$$

9 9

The standard computation of $\det(xI - A) = 0$ shows that $\chi_A(x) = \det(xI - A) = (x-1)^2(x+1)^2$, and so the eigenvalues of A are $1, -1$. We want the minimal polynomial of A, which is given by $\prod(x - \lambda_i)^{\alpha_i}$ where $\alpha_i = \dim E_{\lambda_i}$ is the geometric multiplicity of λ_i.

Another standard computation shows that

$$\lambda = 1 \implies \operatorname{rank}(A - 1I) = 2 \implies \dim\ker(A - 1I) = 4 - 2 = 2$$

and similarly

$$\lambda = -1 \implies \operatorname{rank}(A + I) = 3 \implies \dim\ker(A + I) = 4 - 3 = 1.$$

We thus have

$$\begin{aligned} p_A(x) &= (x-1)(x+1)^2 \\ \chi_A(x) &= (x-1)^2(x+1)^2. \end{aligned}$$

To compute $JCF(A)$, we use the following facts:

- For $\lambda = 1$,
  - Since $(x-1)^1$ occurs in $p_A(x)$, the largest Jordan block for $\lambda = 1$ is size 1.
  - Since $(x-1)^2$ occurs in $\chi_A(x)$, the sum of sizes of all such Jordan blocks is 2.
  - Since $\dim E_1 = 2$, there are 2 such Jordan blocks.
- For $\lambda = -1$,
  - Since $(x+1)^2$ occurs in $p_A(x)$, the largest Jordan block for $\lambda = -1$ is size 2.
  - Since $(x+1)^2$ occurs in $\chi_A(x)$, the sum of sizes of all such Jordan blocks is 2.
  - Since $\dim E_{-1} = 1$, there is 1 such Jordan block.

We can thus immediately write

$$JCF(A) = J_{-1}^2 \oplus 2J_1^1 = \begin{bmatrix} -1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

By arguments similar to the previous two problems, the only possible invariant factor decomposition is given by

$$\begin{aligned} d_1 &= (x+1) \\ d_2 &= (x-1)^2(x+1) \end{aligned}$$

and thus

$$RCF(A) = C(d_1) \oplus C(d_2) = \left[\begin{array}{c|ccc} -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right].$$

10 10

Suppose $A^* = A$. It is then a fact that A is self-adjoint, and so for every $\mathbf{v} \in V$ we have

$$\langle A\mathbf{v},\ \mathbf{v}\rangle = \langle \mathbf{v},\ A^*\mathbf{v}\rangle = \langle \mathbf{v},\ A\mathbf{v}\rangle.$$

10.1 a

Let $(\lambda, \mathbf{v})$ be an eigenvalue of A with one of its corresponding eigenvectors, so $A\mathbf{v} = \lambda\mathbf{v}$.

On one hand,

$$\langle A\mathbf{v},\ \mathbf{v}\rangle = \langle \lambda\mathbf{v},\ \mathbf{v}\rangle = \lambda\langle \mathbf{v},\ \mathbf{v}\rangle = \lambda\|\mathbf{v}\|^2,$$

while on the other hand,

$$\langle A\mathbf{v},\ \mathbf{v}\rangle = \langle \mathbf{v},\ A^*\mathbf{v}\rangle = \langle \mathbf{v},\ A\mathbf{v}\rangle = \langle \mathbf{v},\ \lambda\mathbf{v}\rangle = \overline{\lambda}\langle \mathbf{v},\ \mathbf{v}\rangle = \overline{\lambda}\|\mathbf{v}\|^2.$$

Equating these expressions, we find that

$$\lambda = \overline{\lambda} \implies \lambda \in \mathbb{R}. \blacksquare$$

10.2 b

We can make use of the following fact:

Theorem (Schur): Every square matrix $A \in M_n(\mathbb{C})$ is unitarily similar to an upper triangular matrix, i.e. there exists a unitary matrix U such that $A = UTU^{-1}$ where T is upper-triangular.

Applying this theorem yields $A = UTU^{-1}$ and thus $T = U^{-1}AU$. In particular, $A \sim T$.

Noting that if U is unitary then $U^{-1} = U^*$, we have

$$\begin{aligned} T^* &= (U^{-1}AU)^* \\ &= U^*A^*(U^{-1})^* \\ &= U^*A^*U^{**} \\ &= U^{-1}A^*U \\ &= T, \end{aligned}$$

and so $T^* = T$.

Since T is upper triangular, this forces $T_{ij} = 0$ whenever $i \neq j$ But this makes T diagonal, so A is similar to a diagonal matrix. $\blacksquare$

Proof of Schur's Theorem: We'll proceed by induction on $n = \dim_{\mathbb{C}}(V)$, and showing that there is an orthonormal basis of V such that the matrix of A is upper triangular.

Lemma: If V is finite dimensional and λ is an eigenvalue of A, then $\overline{\lambda}$ is an eigenvalue of A^*.

Proof:

$$\det(A - \lambda I) = 0 = \overline{\det\left(A^* - \bar{\lambda} I\right)}. \blacksquare$$

Since $\mathbb{C}$ is algebraically closed, every matrix $A \in M_n(\mathbb{C})$ will have an eigenvalue, since its characteristic polynomial will have a root by the Fundamental Theorem of Algebra.

So let $\lambda_1, \mathbf{v}_1$ be an eigenvalue/eigenvector pair of the adjoint A^*.

Consider the space $S = \operatorname{span}_{\mathbb{C}} \{\mathbf{v}_1\}$; then $V = S \oplus S^\perp$. The claim is that the original A will restrict to an operator on $S^\perp$, which has dimension $n-1$. The inductive hypothesis will then apply to $A|_{S^\perp}$.

Note that if this holds, there will be an orthonormal basis $\mathcal{B}$ of $S^\perp$ such that the matrix

$$\mathbf{A}' \coloneqq [A|_{S^\perp}]_{\mathcal{B}}$$

will be upper triangular. We would then be able to obtain an orthonormal basis $\mathcal{C} \coloneqq \mathcal{B} \bigcup \{\mathbf{v_1}\}$ of $S \oplus S^\perp = V$.

Since we have a direct sum decomposition, the matrix of A with respect to $\mathcal{C}$ can be written in block form as

$$[A]_{\mathcal{C}} = \begin{bmatrix} [A|_S]_{\mathcal{C}} & 0 \\ 0 & [A|_{S^\perp}]_{\mathcal{C}} \end{bmatrix} = \begin{bmatrix} [A|_S]_{\{\mathbf{v}_1\}} & 0 \\ 0 & [A|_{S^\perp}]_{\mathcal{B}} \end{bmatrix} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \mathbf{A}' \end{bmatrix},$$

which is upper-triangular since $\mathbf{A}'$ is upper-triangular.

To see that A does indeed restrict to an operator on $S^\perp$, we need to show that $A(S^\perp) \subseteq S^\perp$. So let $\mathbf{s} \in S^\perp$; then $\langle \mathbf{v}_1,\ \mathbf{s}\rangle = 0$ by definition. Then $A\mathbf{s} \in S^\perp$ since

$$\begin{aligned}
\langle \mathbf{v}_1,\ A\mathbf{s}\rangle &= \langle A^*\mathbf{v}_1,\ \mathbf{s}\rangle \\
&= \langle \lambda_1 \mathbf{v}_1,\ \mathbf{s}\rangle \\
&= \lambda_1 \langle \mathbf{v}_1,\ \mathbf{s}\rangle \\
&= 0.
\end{aligned}$$

$\blacksquare$