

Homework 6
April 30

1. Compute the kernel and cokernel of the following maps:

a) $\alpha : \mathbb{Z}^{\oplus 2} \rightarrow \mathbb{Z}^{\oplus 3}$ given by

$$\begin{pmatrix} 4 & 2 \\ 1 & 1 \\ 3 & 2 \end{pmatrix}$$

kernel is 0, cokernel is \mathbb{Z}

b) $\beta : \mathbb{Z}^{\oplus 2} \rightarrow \mathbb{Z}^{\oplus 3}$ given by

$$\begin{pmatrix} 5 & 1 & 3 \\ 2 & 1 & 2 \end{pmatrix}$$

kernel is \mathbb{Z} , cokernel is 0.

2. Consider the matrix $A \in M_3(\mathbb{Z})$

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

a) Thinking of A as a linear transformation of \mathbb{Q} vector spaces, find the characteristic and minimal polynomials for A . Find the rational canonical form for A (over \mathbb{Q}).

The characteristic polynomial is $f(x) = x^3 - 3x^2 + x - 5$ which has one real root between 3 and 4 and two complex roots (first semester calculus). Thus, $f(x)$ is irreducible over \mathbb{Z} and hence irreducible over \mathbb{Q} . Since the minimal polynomial shares the same irreducible factors as the characteristic polynomial the minimum polynomial equals the characteristic polynomial and the RCF is a single block,

$$\begin{pmatrix} 0 & 0 & 5 \\ 1 & 0 & -1 \\ 0 & 1 & 3 \end{pmatrix}$$

b) Repeat part a) but now consider A as a linear transformation of $\mathbb{Z}/7$ and $\mathbb{Z}/2$ respectively.

Over $\mathbb{Z}/7$ the characteristic polynomial factors as $f(x) = (x - 2)(x^2 + 6x - 1)$. Since this has no repeated factors, once again the minimum = characteristic polynomial.

Over $\mathbb{Z}/2$, the characteristic polynomial factors as $f(x) = (x - 1)^3$. Thus, the minimum polynomial could be $(x - 1)$, $(x - 1)^2$ or $(x - 1)^3 = f$. However, $\{e_3, A(e_3), A^2(e_3)\}$ is a

basis and hence this is a cyclic $\mathbb{Z}/2[T]$ module structure on $\mathbb{Z}^{\oplus 3}$ and we again have only one RFC block (the minimum polynomial = characteristic polynomial).

c) For which fields is A diagonalizable?

First observe that A is diagonalizable if and only if the minimum polynomial splits into linear factors with no repeated roots (the characteristic polynomial may have repeated roots, but not the minimal polynomial). If our field has characteristic 2, then by part b) the minimum polynomial splits but the matrix is not diagonalizable since it has repeated roots. So we may assume the characteristic is not 2. Doing row/column reductions over $F[T]$ we get

$$\begin{pmatrix} x-2 & -1 & -3 \\ -1 & x & 0 \\ 0 & -2 & x-1 \end{pmatrix} \xrightarrow{\sim} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x^3 - 3x^2 + x - 5 \end{pmatrix}$$

and thus the minimum polynomial equals the characteristic polynomial (there are no non-trivial invariant factors). Thus, A is diagonalizable over F if and only if $f(x) = x^3 - 3x^2 + x - 5$ splits with no repeated roots. Recall that a double root of f is a root of $f'(x) = 3x^2 - 6x + 1$. So, for example, A is diagonalizable in a splitting field of characteristic 3 or characteristic 0. However, not over a field of characteristic 5 since $f(x) = x(x+1)^2$ in this case. If we are not in characteristic 2 or 3, then we see that the roots of $f'(x)$ are $1 + \frac{1}{3}\sqrt{6}$ and $1 - \frac{1}{3}\sqrt{6}$. Plugging these back into f and solving, we find that if these are roots then $25 \cong 0$ in our field. Thus, A will be diagonalizable in F if and only if it is characteristic not equal to 2 or 5 and contains the splitting field of f over \mathbb{Z}/p or \mathbb{Q} .

3. Let $n = p^t$ for p a prime integer.

a) Let F be a field and $f \in F[x]$ of degree k . Prove that if f splits in a Galois extension of F of degree n such that $\gcd(k,n) = 1$ then f has a root in F .

If we write f as a product of irreducible polynomials, then since f splits in a Galois extension of order p^t , each irreducible factor of f of degree greater than 1 must have degree divisible by p . Since $\gcd(k,n) = 1$ and k is the sum of the degrees of the irreducible factors at least one of these factors must have degree 1.

b) Let $\gamma : V \rightarrow V$ be a F -module homomorphism of a vector space of dimension k such that the minimal polynomial of $\gamma \otimes_F F'$ splits for F' a Galois extension of F of degree n with $\gcd(k,n) = 1$. Prove that γ has an eigenvector.

Since the minimum polynomial divides the characteristic polynomial, we know by part (a) that the characteristic polynomial of γ has a root, say η , in F . Then $\det(\eta \cdot I - \gamma) = 0$ so $\eta \cdot I - \gamma$ has a kernel of dimension at least one. Any non-trivial vector in this kernel is thus an eigenvector for γ with eigenvalue η .

c) Let F be a field whose algebraic closure is a finite Galois extension of degree n (for example, \mathbb{R}). Let G be a finite group whose order is divisible in F . Let M be a simple left

$F[G]$ module which has dimension k prime to n . Prove that $\text{Hom}_{F[G]}(M, M) \cong F$. (Hint, Schur's lemma, strong form).

You want to show that every $\alpha \in \text{Hom}_{F[G]}(M, M)$ is multiplication by a scalar. If α is not zero, then by (b) it has an eigenvalue η , but then $\alpha - \eta \cdot I$ is a $F[G]$ morphism of M , M simple implies the kernel is 0 or all of M .

d) As in c), we know that $F[G]$ is ring isomorphic to a finite product of matrix rings of division algebras, say $M_{n_1}(D_1) \times \cdots \times M_{n_t}(D_t)$, each of which is an F -algebra. Prove that if $\dim_F(D_i)$ is prime to n , then $D_i \cong F$ in this decomposition.

This is simply a restatement of (c) since each D_i of the decomposition is $\text{Hom}_{F[G]}(M, M)$ for M a simple $F[G]$ module.

4 Suppose we have a condition \mathcal{P} which the modules of a ring R may or may not satisfy (for example, \mathcal{P} could be the condition “the module is finitely generated”, then $M \in \mathcal{P}(R)$ means that M is a finitely generated R -module). Suppose that for every short exact sequence of R -modules,

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

$$(p) \quad A \in \mathcal{P}(R) \text{ and } C \in \mathcal{P}(R) \implies B \in \mathcal{P}(R)$$

(a) Suppose in addition that we assume $B \in \mathcal{P}(R) \implies C \in \mathcal{P}(R)$. Prove that in this case, $R \in \mathcal{P}(R) \iff M \in \mathcal{P}(R)$ for every finitely generated R -module M .

For parts (a) and (d), one inducts up to show that $B = R^{\oplus n}$ satisfies $\mathcal{P}(R)$ for all n .

(b) Prove that the statement $\mathcal{P} =$ “every quotient object is projective” satisfies (p) + (d). Prove that in this case $R \in \mathcal{P}(R) \iff R$ is semi-simple.

For parts (b) and (c) one uses pushouts. If $B \rightarrow X$ is a quotient, then we get

$$\begin{array}{ccccccccc} 0 & \rightarrow & A & \rightarrow & B & \rightarrow & C & \rightarrow & 0 \\ & & \downarrow \cong & & \downarrow & & \downarrow & & \\ 0 & \rightarrow & A & \rightarrow & X & \rightarrow & PO & \rightarrow & 0 \end{array}$$

with the map from $C \rightarrow PO$ a quotient.

For the second part, one uses that every subobject splits, i.e. left ideal of R .

(c) Prove that the statement $\mathcal{P} =$ “every quotient object is injective” satisfies (p) + (d). Prove that a domain R satisfies this condition if and only if it is a field.

Since R is a domain, we simply need to show that multiplication by a non-zero element a is surjective. Since R/aR is injective, there is an R -module map $\phi : R \rightarrow R/aR$ such that

$\phi \circ (a \cdot -)$ is the quotient map from R . But then $\phi(a \cdot x) = a\phi(x) = 0$ so $R/aR = 0$ and hence multiplication by a is an isomorphism.

(d) Suppose we now assume the different additional hypothesis that $B \in \mathcal{P}(R) \implies A \in \mathcal{P}(R)$. Prove that in this case, $R \in \mathcal{P}(R) \iff$ every submodule of a finitely generate free R -module is in $\mathcal{P}(R)$.

(e) Prove that the statement $\mathcal{P} =$ “every submodule is free” satisfies (a) + (p). Prove that a Noetherian domain R satisfies this condition $\iff R$ is a PID.

Since R is Noetherian, every submodule is finitely generated. Since R is a domain, it is a commutative ring so every ideal is a free submodule of finite rank but by considering the exterior power functor it must have rank no more than 1, i.e. the ideal is generated by one element.

(f) Prove that the statement $\mathcal{P} =$ “every submodule is injective” satisfies (a)+ (p). Prove that a ring R satisfies $\mathcal{P} \iff R$ is semi-simple.