University of New South Wales

School of Mathematics and Statistics

Assignment 2

Modules and Representation Theory

Author:
Edward McDonald

Student Number:
3375335

Question 1

Let $R = \mathbb{R}[x]$.

Lemma 1. *Let K be the submodule of R^2 generated by*

$$\begin{pmatrix} x+x^2 \\ 2x+x^2 \end{pmatrix}, \begin{pmatrix} 2x+x^2 \\ 4x+x^2 \end{pmatrix}.$$

Then

$$R^2/K = \frac{\mathbb{R}[x]}{\langle x \rangle} \oplus \frac{\mathbb{R}[x]}{\langle x^2 \rangle} \cong \mathbb{R} \oplus \frac{\mathbb{R}}{\langle x^2 \rangle}$$

Proof. We consider the matrix

$$\begin{pmatrix} x+x^2 & 2x+x^2 \\ 2x+x^2 & 4x+x^2 \end{pmatrix}$$

This is simply

$$x \begin{pmatrix} 1+x & 2+x \\ 2+x & 4+x \end{pmatrix}$$

Subtracting twice the first row from the second, this becomes

$$x \begin{pmatrix} 1+x & 2+x \\ 1 & 2 \end{pmatrix}.$$

Now subtract $(1+x)$ times the second row from the first,

$$x \begin{pmatrix} 0 & -x \\ 1 & 2 \end{pmatrix}.$$

Now subtract the twice the first column from the second, and we obtain

$$\begin{pmatrix} 0 & -x^2 \\ x & 0 \end{pmatrix}.$$

Hence, the image of the matrix

$$\begin{pmatrix} x & 0 \\ 0 & -x^2 \end{pmatrix}$$

generates a submodule N, such that

$$R^2/K \cong R^2/N.$$

Hence,

$$R^2/K \cong \frac{R^2}{Rx \oplus Rx^2} \cong R/\langle x \rangle \oplus R/\langle x^2 \rangle.$$

□

Proposition 1. *Suppose that $p_1(x), p_2(x), p_3(x), p_4(x) \in R$. Suppose that N is the submodule of R^2 generated by*

$$\begin{pmatrix} p_1 \\ p_2 \end{pmatrix}, \begin{pmatrix} p_3 \\ p_4 \end{pmatrix}$$

Let $d(x)$ be the determinant of

$$\begin{pmatrix} p_1(x) & p_3(x) \\ p_2(x) & p_4(x) \end{pmatrix}$$

Then R^2/N is infinite dimensional as a real vector space if and only if $d(x) = 0$. Otherwise,

$$\dim(R^2/N) = \deg d(x).$$

Proof. There exist matrices Φ_l and Φ_r in $M_n(R)$ such that

$$\Phi_l \begin{pmatrix} p_1(x) & p_3(x) \\ p_2(x) & p_4(x) \end{pmatrix} \Phi_r = \begin{pmatrix} q_1(x) & 0 \\ 0 & q_2(x) \end{pmatrix}$$

where $\det(\Phi_l), \det(\Phi_r) \neq 0$ and $q_1|q_2$. So,

$$d(x) = \det \begin{pmatrix} p_1(x) & p_3(x) \\ p_2(x) & p_4(x) \end{pmatrix} = \det(\Phi_l)^{-1} \det(\Phi_r)^{-1} q_1(x) q_2(x)$$

and

$$R^2/N \cong \frac{R^2}{Rq_1(x) \oplus Rq_2(x)} \cong R/\langle q_1(x) \rangle \oplus R/\langle q_2(x) \rangle.$$

If $d(x) = 0$, then $q_1(x) = 0$ or $q_2(x) = 0$. Hence, in the case $d(x) = 0$, $R^2/N \cong R \oplus R/\langle q_2(x) \rangle$ or $R^2/N \cong R/\langle q_1(x) \rangle \oplus R$. So R^2/N has infinite real dimension if $d(x) = 0$ since R is infinite dimensional.

If $d(x) \neq 0$, then $q_1(x) \neq 0$ and $q_2(x) \neq 0$. In this case, R^2/N must be finite dimensional since $R/\langle q_1(x) \rangle$ and $R/\langle q_2(x)$ are spanned by monomials $1, x, x^2, \dots, x^n$ for $n \leq \deg(q_1)$ and $n \leq \deg(q_2)$ respectively.

Hence R^2/N is infinite dimensional if and only if $d(x) = 0$.

If $R/\langle q_1(x) \rangle$ is finite dimensional, then it has real dimension $\deg(q_1)$ since if $f(x) \in R$, then $f(x) = q(x)q_1(x) + r(x)$, where $\deg(r) < \deg(q_1)$, so r is a linear combination of $1, x, x^2, \dots, x^n$ for $n < \deg(q_1)$. Hence these are $\deg(q_1)$ linearly independent spanning elements of $R/\langle q_1(x) \rangle$.

Similarly, if $R/\langle q_2(x) \rangle$ is finite dimensional, then it has real dimension $\deg(q_2)$.

Hence, if R^2/N has finite real dimension,

$$\dim_{\mathbb{R}}(R^2/N) = \deg(q_1) \deg(q_2) = \deg(d).$$

□

Question 2

In this question, we consider the algebra $A = \mathbb{F}_3 G$ where $G = \langle \sigma \rangle$ is the cyclic group of order 4. We use the isomorphism,

$$A \cong \frac{\mathbb{F}_3[x]}{\langle x^4 - 1 \rangle}, \quad \sigma \mapsto x$$

Note that $x^4 - 1 = (x-1)(x+1)(x^2+1)$. This is a decomposition into prime factors, since $x - 1$ and $x + 1$ are degree 1, and therefore prime, and if $x^2 + 1$ has a proper factor, then it has a linear factor. If $x^2 + 1$ has a linear factor, it has a root over $\mathbb{F}_3$. However for $x \in \mathbb{F}_3$, $x^2 + 1 \neq 0$.

Lemma 2. *The maximal ideals of A are exactly*

$$\begin{aligned} &\langle \sigma - 1 \rangle \\ &\langle \sigma + 1 \rangle \\ &\langle \sigma^2 + 1 \rangle. \end{aligned}$$

Proof. Ideals of $\mathbb{F}_3[x]/\langle x^4 - 1 \rangle$ are of the form $\langle f(x) \rangle / \langle x^4 - 1 \rangle$ for some $f(x) | x^4 - 1$. An ideal $\langle f(x) \rangle / \langle x^4 - 1 \rangle$ is maximal if and only if

$$\frac{\mathbb{F}_3[x]/\langle x^4 - 1 \rangle}{\langle f(x) \rangle / \langle x^4 - 1 \rangle} \cong \frac{\mathbb{F}_3[x]}{\langle f(x) \rangle}$$

is a field. That is, $f(x)$ must be an irreducible divisor of $x^4 - 1$. Hence we have three choices for $f(x)$:

$$\begin{aligned} &x^2 + 1 \\ &x - 1 \\ &x + 1. \end{aligned}$$

So in A, this corresponds to $\sigma^2 + 1$, $\sigma - 1$ or $\sigma + 1$. Hence the required maximal ideals are $\langle \sigma^2 + 1 \rangle, \langle \sigma - 1 \rangle, \langle \sigma + 1 \rangle$. □

Theorem 1. *A has Wedderburn decomposition,*

$$A \cong \frac{\mathbb{F}_3[x]}{\langle x - 1 \rangle} \times \frac{\mathbb{F}_3[x]}{\langle x + 1 \rangle} \times \frac{\mathbb{F}_3[x]}{\langle x^2 + 1 \rangle} \cong \mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_9.$$

Proof. This follows from the Chinese remainder theorem, since $A \cong \mathbb{F}_3[x]/\langle x^4 - 1 \rangle$, and the ideals

$$\begin{aligned} &\langle x - 1 \rangle \\ &\langle x + 1 \rangle \\ &\langle x^2 + 1 \rangle. \end{aligned}$$

generate $\mathbb{F}_3[x]$, are generated by coprime polynomials and have intersection $\langle x^4-1\rangle$, we have

$$A \cong \frac{\mathbb{F}_3[x]}{\langle x^4-1\rangle} \cong \frac{\mathbb{F}_3[x]}{\langle x-1\rangle} \times \frac{\mathbb{F}_3[x]}{\langle x+1\rangle} \times \frac{\mathbb{F}_3[x]}{\langle x^2+1\rangle} \cong \mathbb{F}_3 \times \mathbb{F}_3 \times \mathbb{F}_9.$$

$\square$

Lemma 3. *The Wedderburn decomposition in theorem 1 corresponds to an isomorphism*

$$\frac{\mathbb{F}_3[x]}{\langle x-1\rangle} \times \frac{\mathbb{F}_3[x]}{\langle x+1\rangle} \times \frac{\mathbb{F}_3[x]}{\langle x^2+1\rangle} \cong \frac{\mathbb{F}_3[x]}{\langle x^4-1\rangle}$$

given by

$$(a(x), b(x), c(x)) \mapsto a(x)(x+1)(x^2+1) - b(x)(x-1)(x^2+1) + c(x)(x-1)(x+1).$$

Proof. The isomorphism

$$\frac{\mathbb{F}_3[x]}{\langle x^4-1\rangle} \to \frac{\mathbb{F}_3[x]}{\langle x-1\rangle} \times \frac{\mathbb{F}_3[x]}{\langle x+1\rangle} \times \frac{\mathbb{F}_3[x]}{\langle x^2+1\rangle}$$

is given by

$$f(x) \mapsto (f(x) + \langle x-1\rangle, f(x) + \langle x+1\rangle, f(x) + \langle x^2+1\rangle).$$

So we wish to find $e_1(x), e_2(x), e_3(x) \in \mathbb{F}_3[x]/\langle x^4-1\rangle$ such that $e_1(x) \mapsto (1,0,0)$, $e_2(x) \mapsto (0,1,0)$ and $e_3(x) \mapsto (0,0,1)$ under this isomorphism.

So we require $e_1(x) \in \langle x+1\rangle \cap \langle x^2+1\rangle$, and $e_1(x) + \langle x-1\rangle = 1 + \langle x-1\rangle$. The only choice for $e_1(x)$ is $(x+1)(x^2+1)$.

Similarly, $e_2(x) = -(x-1)(x^2+1)$ and $e_3(x) = (x-1)(x+1)$.

Hence, the isomorphism

$$\frac{\mathbb{F}_3[x]}{\langle x-1\rangle} \times \frac{\mathbb{F}_3[x]}{\langle x+1\rangle} \times \frac{\mathbb{F}_3[x]}{\langle x^2+1\rangle} \to \frac{\mathbb{F}_3[x]}{\langle x^4-1\rangle}$$

maps $(1,0,0)$ to $e_1(x)$, $(0,1,0)$ to $e_2(x)$ and $(0,0,1)$ to $e_3(x)$, and so by $\mathbb{F}_3[x]$-linearity, the result follows. $\square$

Definition 1. *Let $\rho : G \to \mathrm{GL}_3(\mathbb{F}_3)$ be the $\mathbb{F}_3$-linear representation of G given by*

$$\rho(\sigma) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ -1 & 1 & 0 \end{pmatrix}$$

The corresponding $\mathbb{F}_3G$-module $V = {\mathbb{F}_3}^3$ is defined for $v \in V$ by

$$\left(\sum_{g\in G} \alpha_g g\right) v = \sum_{g\in G} \alpha_g \rho(g) v$$

See that

$$\rho(\sigma)^2 = \rho(\sigma^2) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & -1 & 0 \\ -1 & 0 & -1 \end{pmatrix}$$

Hence,

$$\begin{aligned}(\sigma^2 - 1)\begin{pmatrix}1\\1\\0\end{pmatrix} &= (\rho(\sigma)^2 - I)\begin{pmatrix}1\\1\\0\end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix}\begin{pmatrix}1\\1\\0\end{pmatrix} \\ &= \begin{pmatrix}0\\-1\\-1\end{pmatrix}\end{aligned}$$

Proposition 2. *If $\langle f(x)\rangle/\langle x^4 - 1\rangle$ is a maximal ideal of $\mathbb{F}_3[x]/\langle x^4 - 1\rangle$, then this corresponds to a maximal ideal $\langle f(\sigma)\rangle$ of A and the corresponding isotypic component of V is $\ker f(\rho(\sigma))$.*

Proof. The isotypic components of V correspond to the images of left multiplication by the multiplicative identities in each Wedderburn component. In the notation of lemma 3, this means that the isotypic components are

$$\begin{gathered} e_1(\rho(\sigma))V \\ e_2(\rho(\sigma))V \\ e_3(\rho(\sigma))V. \end{gathered}$$

To find the image of $e_1(\rho(\sigma))$, note that since

$$V = e_1(\rho(\sigma))V + e_2(\rho(\sigma))V + e_3(\rho(\sigma))V$$

we may write

$$\begin{aligned}\mathrm{im} e_1(\rho(\sigma)) &= \ker e_2(\rho(\sigma)) \cap \ker e_3(\rho(\sigma)) \\ &= \ker(\rho(\sigma) - I)(\rho(\sigma)^2 + I) \cap \ker(\rho(\sigma) - I)(\rho(\sigma) + I)\end{aligned}$$

It is clear that $\ker\rho(\sigma)-I \subset \ker(\rho(\sigma)-I)(\rho(\sigma)^2+I)\cap\ker(\rho(\sigma)-I)(\rho(\sigma)+I)$, and the opposite inclusion holds because $I = \rho(\sigma)^2+I-\rho(\sigma)(\rho(\sigma)+I)$.

Similarly,

$$\begin{aligned} e_1(\rho(\sigma))V &= \ker(\rho(\sigma)-I) \\ e_2(\rho(\sigma))V &= \ker(\rho(\sigma)+I) \\ e_3(\rho(\sigma))V &= \ker(\rho(\sigma)^2+I). \end{aligned}$$

□

Remark 1. *The preceding result states that*

$$V = \ker(\rho(\sigma)-I)\oplus\ker(\rho(\sigma)+I)\oplus\ker(\rho(\sigma)^2+I)$$

An identical decomposition could be obtained by primary decomposition, since

$$(\rho(\sigma)^2+I)(\rho(\sigma)+I)(\rho(\sigma)-I) = 0$$

and the polynomials

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

are coprime.

Corollary 1. *Hence the isotypic components of V are*

$$\mathbb{F}_3\begin{pmatrix}-1\\1\\-1\end{pmatrix},\quad \mathbb{F}_3\begin{pmatrix}0\\1\\0\end{pmatrix}\oplus\mathbb{F}_3\begin{pmatrix}0\\0\\1\end{pmatrix},\quad 0.$$

Proof. $\ker(\rho(\sigma)-I)$ is simply

$$\ker\begin{pmatrix}0&0&0\\0&-1&-1\\-1&1&-1\end{pmatrix} = 0.$$

Similarly, $\ker(\rho(\sigma)+I)$ is

$$\ker\begin{pmatrix}-1&0&0\\0&1&-1\\-1&1&1\end{pmatrix} = \mathbb{F}_3\begin{pmatrix}-1\\1\\-1\end{pmatrix}$$

And $\ker(\rho(\sigma)^2+I)$ is

$$\ker\begin{pmatrix}-1&0&0\\1&0&0\\-1&0&0\end{pmatrix} = \mathbb{F}_3\begin{pmatrix}0\\0\\1\end{pmatrix}\oplus\mathbb{F}_3\begin{pmatrix}0\\1\\0\end{pmatrix}$$

□

Question 3

For this question, $G = \langle \sigma, \tau \mid \sigma^3 = 1, \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle$, and $A = \mathbb{F}_3 G$.

Theorem 2. *There are two one dimensional representations of G in $\mathbb{F}_3$, given by*

$$\sigma \mapsto 1,\ \tau \mapsto 1$$
$$\sigma \mapsto 1,\ \tau \mapsto -1$$

Proof. If $f : G \to {\mathbb{F}_3}^\times = \{1, -1\}$ is a one dimensional representation, it must have $f(\sigma) = 1$, since $f(\sigma)^3 = f(\sigma)^3 = 1$. Then we may choose $f(\tau) = 1$ or $f(\tau) = -1$. Since $\rho(\tau)^2 = (-1)^2 = 1$, and $\rho(\tau)\rho(\sigma) = \rho(\sigma)^{-1}\rho(\tau)$, this uniquely determines the representation by the universal property of free groups.

Hence there are exactly two one dimensional representations of G, given as above. ☐

Alternatively, we could have computed the abelianisation $G_{ab} = \langle\ \sigma, \tau | \tau^2 = \sigma^2 = 1,\ \tau\sigma = \sigma\tau\ \rangle$ and found $\mathrm{Hom}_{\mathbb{Z}}(G_{ab}, {\mathbb{F}_3}^\times)$.

Definition 2. *The representation $\rho : G \to \mathrm{GL}_2(\mathbb{F}_3)$ is given by*

$$\rho(\sigma) = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},\ \ \rho(\tau) = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$$

$V = {\mathbb{F}_3}^2$ is the corresponding A-module.

Proposition 3. *V is not semi-simple.*

Proof. Consider the subspace $\mathbb{F}_3 v$, where

$$v = \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

$\mathbb{F}_3 v$ is an A-submodule of V, since $\rho(\sigma)v = v$ and $\rho(\tau)v = -v$.

If V is semi-simple, then $\mathbb{F}_3 v$ must be a direct summand of V. Hence there is another submodule $\mathbb{F}_3 u$ for some u not parallel to v such that $V = \mathbb{F}_3 v + \mathbb{F}_3 u$.

However if $\mathbb{F}_3 u$ is a submodule of V, then u must be an eigenvector of $\rho(\sigma)$.

However, the characteristic polynomial of $\rho(\sigma)$ is $\mathrm{cp}_{\rho(\sigma)}(\lambda) = (\lambda - 1)^2$, and $\ker \rho(\sigma) - I = \mathbb{F}_3 v$.

Hence $\rho(\sigma)$ has no eigenvectors other then v, and so $\mathbb{F}_3 v$ cannot be a direct summand of V. Hence V is not semi-simple. ☐

Proposition 4. *A composition series for V is*

$$0 < \mathbb{F}_3 v < V$$

where $v = (1, -1)^\top$ as in proposition 3. The composition factors are

$$\mathbb{F}_3 v, V/\mathbb{F}_3 v$$

which are isomorphic as $\mathbb{F}_3$ modules to $\mathbb{F}_3$, but as A modules they correspond to the representations in theorem 2.

Proof. We have already shown in proposition 3 that $\mathbb{F}_3 v$ is an A-submodule of V. So it is required to show that $0 < \mathbb{F}_3 v < V$ is a composition series, by showing that the composition factors are simple.

The A-modules

$$\mathbb{F}_3 v/0, \;\; V/\mathbb{F}_3 v$$

are simple, since they are one dimensional as vector spaces over $\mathbb{F}_3$, hence can have no nontrivial A-submodules.

These composition factors are one dimensional $\mathbb{F}_3$-vector spaces, and A-modules, so correspond to one dimensional representations of G.

See that since $\rho(\sigma)v = v$ and $\rho(\tau)v = -v$, the first composition factor $\mathbb{F}_3 v/0$ corresponds to the nontrivial representation in theorem 2.

For $u + \mathbb{F}_3 v \in V/\mathbb{F}_3 v$, the action of g on $u + \mathbb{F}_3 v$ is given by $\rho(g)(u) + \mathbb{F}_3 v$. This is well defined since v is an eigenvector of $\rho(\sigma)$ and $\rho(\tau)$, so $\mathbb{F}_3 v$ is invariant under the action of G.

Elements of $V/\mathbb{F}_3 v$ can be described as

$$\alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \mathbb{F}_3 v$$

for some $\alpha \in \mathbb{F}_3$ since if $u + \mathbb{F}_3 v$ is any coset of $\mathbb{F}_3 v$, then we may find $\alpha \in \mathbb{F}_3$ such that $u + \mathbb{F}_3 v = \alpha(1, 0)^\top + \mathbb{F}_3 v$.

Hence, for any $\alpha(1, 0)^\top + \mathbb{F}_3 v \in V/\mathbb{F}_3 v$, we may compute

$$\rho(\sigma)(\alpha(1,0)^\top + \mathbb{F}_3 v) = \alpha(1,0) + \mathbb{F}_3 v$$
$$\rho(\tau)(\alpha(1,0)^\top + \mathbb{F}_3 v) = \alpha(1,0) + \mathbb{F}_3 v$$

So this corresponds to the trivial representation in theorem 2.

□

Remark 2. *The composition factors in the above proposition are isomorphic to the simple A modules induced by the representations in theorem 2 since they induce the same G-representation.*