Math 210C Algebra: Final

June 12th, 2019

Professor Sharifi

Anish Chedalavada

Problem 1

Let R be a commutative ring, $\mathfrak{p}$ a prime ideal, and n a positive integer.

a.i) **WTS** The ideal $\mathfrak{p}^{(n)} = R \cap \mathfrak{p}^n R_{\mathfrak{p}}$ is $\mathfrak{p}$-primary.

Proof. $R \cap \mathfrak{p}^n R_{\mathfrak{p}} = \{r \in R \mid \exists\ s, t \in R \setminus \mathfrak{p} \text{ s.t. } trs \in \mathfrak{p}^n\}$ i.e. the set of $r \in R$ s.t. there is some $s \in R \setminus \mathfrak{p} = S$ with $sr \in \mathfrak{p}^n$. Suppose $r \in \sqrt{p^{(n)}}$. Then $r^n s \in \mathfrak{p}^n$ for some n, $s \in S \implies r^{nk} \in \mathfrak{p}$ some k as $s \notin \mathfrak{p}$. In particular, $r \in \mathfrak{p}$, and so $\sqrt{\mathfrak{p}^{(n)}} \subseteq \mathfrak{p}$, but it must also contain $\mathfrak{p}$ as $\mathfrak{p}^n \subset \mathfrak{p}^{(n)}$. Thus, $\sqrt{\mathfrak{p}^{(n)}} = \mathfrak{p}$ and we have the result. □

a.ii) **WTS** Suppose that $\mathfrak{p}^n$ has a minimal primary decomposition Q. Show that $\mathfrak{p}^n \in Q$.

Proof. Let $r \in \mathfrak{p}^{(n)}$, $s \in R \setminus \mathfrak{p} = S$ s.t. $sr \in \mathfrak{p}^n$. In particular, for any primary ideal $\mathfrak{q}$ in Q, $sr \in \mathfrak{q} \implies r \in \mathfrak{q}$ as $s^n \notin \mathfrak{q}$ as $s \in S$ and thus $s^n \notin \mathfrak{p}$. Thus, $\mathfrak{p}^{(n)} \subset \mathfrak{q}$ for any primary ideal in Q, implying that $\mathfrak{p}^{(n)}$ must be in a minimal primary decomposition of $\mathfrak{p}^n$ as every primary ideal in Q contains it and it contains $\mathfrak{p}^n$. □

b. Suppose that R is Noetherian, and Q a minimal primary decomposition of (0). Let $\mathfrak{p}$ be an associated prime of (0), and let $\mathfrak{q}$ be $\mathfrak{p}$-primary.

b.i) **WTS** $\mathfrak{p}^{(n)} \subset \mathfrak{q}$ for sufficiently large n.

Proof. As $\mathfrak{p}$ is finitely generated with generators $(p_1, ..., p_n)$ and we have that $p_i^{n_i} \in \mathfrak{q}$ for n_i sufficiently large, we know that we may select $N >> n_i$ such that $a^N \mathfrak{q}\ \forall a \in \mathfrak{p}$, as for any sum $a = r_1 p_1 + ... + r_n p_n$ there is a number N such that every monomial of p_is in a^N has exponent greater than n_i by the binomial theorem. Furthermore, for $M >> N$, all any elements in $\mathfrak{p}^N$ must be a sum of monomials in $p_1, ..., p_n$ with each monomial containing at least one term with exponent greater than N and thus lying in $\mathfrak{q}$ as any element is expressible as $r_1 p_1 + ... + r_n p_n$ and thus for $N > n$ all terms have at least one p_i with exponent greater than 1, and we apply this iteratively. This implies that for M sufficiently large, $\mathfrak{p}^M \subset \mathfrak{q} \implies \mathfrak{p}^{(M)} \subseteq \mathfrak{q}$ by the logic in part a.ii). □

b.ii) **WTS** Suppose $\mathfrak{p}$ is isolated. Show that $R_{\mathfrak{p}}$ is artinian and $\mathfrak{q} = \mathfrak{p}^{(n)}$ for some n.

Proof. If $\mathfrak{p}$ is an isolated prime of (0) then it is in particular a minimal prime of R, and thus $R_{\mathfrak{p}}$ has only one prime ideal, i.e. the unique maximal ideal $\mathfrak{p}R_{\mathfrak{p}} = \mathfrak{m}$, and thus this must be the nilradical as the nilradical is the intersection of all prime ideals. Furthermore, this maximal ideal is finitely generated by elements $(p_1, ..., p_n)$, and thus by the logic used in *b.i)* there is an M sufficiently large such that $(\mathfrak{m})^M = 0$. Consider the ideal $\mathfrak{m}/\mathfrak{m}^2$. We have that $R_{\mathfrak{p}}/\mathfrak{m}^2$ has no nonmaximal prime ideals. Note in the ideal $\mathfrak{m}/\mathfrak{m}^2 = (l_1, ..., l_s)/$ we have that any product of the form $l_i l_j = 0$. Thus the ideal $(l_n) = \{rl_n \mid \text{r is a unit }\}$, and it cannot be prime as there are no nonmaximal prime ideals. Thus, there must be $r, r_1, ..., r_{n-1}, s \in (R_{\mathfrak{p}}/\mathfrak{m}^2)^\times$, s.t. $r \sum_{j=1}^{n-1} r_j l_j = s l_i \implies s^{-1} r \sum_{j=1}^{n-1} r_j l_j = l_i$. In this way, we have eliminated one of the generators of $\mathfrak{m}/\mathfrak{m}^2$ and we may iterate this process until all but one generator has been eliminated, implying $\mathfrak{m}/\mathfrak{m}^2$ is simple and generated by one element.

Thus, in $R_{\mathfrak{p}}$, we have that any element $\pi \in \mathfrak{m} - \mathfrak{m}^2$ must generate all of $\mathfrak{m}$ as there are no ideals properly contained in $\mathfrak{m}$ other than $\mathfrak{m}^2$. Thus, $\mathfrak{m}$ is principally generated by (π). Assume I is an ideal of $R_{\mathfrak{p}}$ not equal to $\mathfrak{m}^k$ some k. Then for any ideal I, we let m maximal s.t. $(pi)^m$ maximally contained in I (exists as (π) is nilpotent). Let $r_1 \pi^k + ... + r_j \pi^j \in I - (\pi)^m$. Factoring out the largest power of π, say j possible from this sum, we get some sum of multiple of π and 1, and this must be a unit as it is not contained in the maximal ideal (π). By assumption, $j < m$ as m s.t. $(\pi)^m \subset I$. However, we have just shown that $r\pi^j \in I$ for r a unit, which is a contradiction. Thus, $I = \mathfrak{m}^k$ some k. In particular, any descending chain of ideals must be of the

form $(\pi)^k \supset ... \supset (\pi)^m$, which always stabilizes as (π) is nilpotent. This yields the claim that $R_{\mathfrak{p}}$ is artinian.

Note then that the symbolic powers $\mathfrak{p}^m$ stabilize for large m. For sufficiently large m, we have that $\mathfrak{p}^{(m)} \subset \mathfrak{q}$ from part i). As the primary ideal associated to an isolated prime in a minimal decomposition is unique (Corollary 11.6.22 of course notes), and

$$(0) \subset \mathfrak{p}^{(m)} \subset \mathfrak{q},\ (0) = \mathfrak{q} \cap \bigcap_{\mathfrak{a} \in Q} \mathfrak{a} \implies (0) = \mathfrak{p}^m \cap \bigcap_{\mathfrak{a} \in Q} \mathfrak{a}$$

So we have that $\mathfrak{q} = \mathfrak{p}^{(m)}$. □

b.iii) **WTS** Suppose that $\mathfrak{p}$ is embedded. Show that if we replace $\mathfrak{q}$ by $\mathfrak{p}^{(n)}$ for any n sufficiently large, then the resulting set is also a minimal primary decomposition of (0).

Proof. Consider the ideal

$$(0) \subset \mathfrak{q} = \mathfrak{q} \cap \bigcap_{\mathfrak{a} \in Q} \mathfrak{a}$$

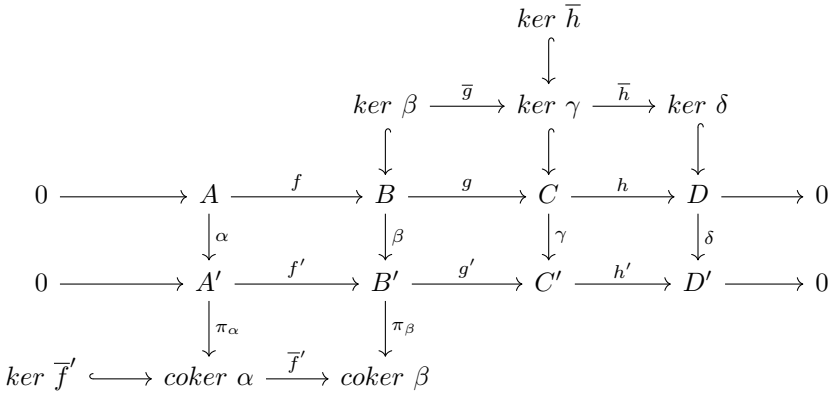
For sufficiently large m, $\mathfrak{p}^{(m)} \subset \mathfrak{q}$, and it is clear that $\mathfrak{p}^m \subset \mathfrak{p}^n$ for $m > n$ as $\mathfrak{p}^m \subset \mathfrak{p}^n \subset \mathfrak{p}^{(n)}$ primary. As before, we have

$$(0) \subset \mathfrak{p}^{(m)} \subset \mathfrak{q},\ (0) = \mathfrak{q} \cap \bigcap_{\mathfrak{a} \in Q} \mathfrak{a} \implies (0) = \mathfrak{p}^m \cap \bigcap_{\mathfrak{a} \in Q} \mathfrak{a}$$

Which in particular implies that $\mathfrak{q}$ can be replace by any $\mathfrak{p}^m$ for m sufficiently large. As minimal decompositions are irredundant, i.e. the primes associated to each primary ideals are distinct, this decomposition is still minimal as all the associated primes are represented exactly once in the replaced decomposition. □

Problem 2

Consider the following diagram where the two longest rows are exact:



WTS ∃ an exact sequence of the form:

$$0 \longrightarrow im\ \overline{g} \longrightarrow ker\ \overline{h} \longrightarrow ker\ \overline{f} \longrightarrow 0$$

Proof. Note that $h \circ g = 0$ by exactness, and thus $h \circ g|_{ker\ \beta} : ker\ \beta \to D = 0$, implying that $\overline{h} \circ \overline{g} : ker\ \beta \to$ ker δ is the zero map, i.e. that $im\ \overline{g} \subset ker\ \overline{h}$. Thus, we have an exact sequence of the form $0 \to im\ \overline{g} \to ker\ \overline{h}$ via the first isomorphism theorem. Now, we define a map $\delta : ker\ \overline{h} \to ker\ \overline{f}'$ in the following manner:

We note firstly that $ker\ \overline{h} \hookrightarrow ker\ h \subset C$ by definition. Let $a \in ker\ \overline{h} \implies a \in im\ g$ by exactness. Thus, we may select a representative in the g-preimage of a, $\widetilde{a} \in B$ (Note: from here onwards the tilde is used as notation for selecting a representative in the g-preimage of some element). Applying β, we have that $\beta(\widetilde{a}) \in ker\ g'$ as $g' \circ \beta(\widetilde{a}) = \gamma \circ g(\widetilde{a}) = \gamma(a) = 0$. By exactness and the fact that f' is monic, we have a unique representative $f'^{-1}(\beta(\widetilde{a})) \in A'$. From here, we may apply π_α, and clearly $\pi(f'^{-1}(\beta(\widetilde{a}))) \in A' \in ker\ \overline{f}'$ as $\overline{f}(\pi(f'^{-1}(\beta(\widetilde{a})))) = \pi_\beta(\beta(\widetilde{a})) = 0$.

We must now show that this is a well-defined process. Let $a = b \in ker\ \overline{h}$. Let $\widetilde{a}, \widetilde{b} \in B$ be lifts in the g-preimage of a, b. We have that $g(\widetilde{a} - \widetilde{b}) = a - b = 0 \implies \widetilde{a} - \widetilde{b} \in ker\ g = im\ f$. Let $k = f^{-1}(\widetilde{a} - \widetilde{b})$, which is well-defined as f monic. W.h.t. $\beta \circ f(k) = f' \circ \alpha(k)$ so $f'^{-1}(\beta(f(k))) = \alpha(k)$. As $\pi_\alpha(f'^{-1}(\beta(f(k)))) = \pi_\alpha(\alpha(k)) = 0 \implies \pi_\alpha(f'^{-1}(\beta(\widetilde{a} - \widetilde{b}))) \implies \pi_\alpha(f'^{-1}(\beta(\widetilde{a}))) - \pi_\alpha(f'^{-1}(\beta(\widetilde{b}))) = 0$ and thus that $a = b \implies \pi_\alpha(f'^{-1}(\beta(\widetilde{a}))) = \pi_\alpha(f'^{-1}(\beta(\widetilde{b})))$ for arbitrary choices of representatives. Note that this map respects the module structure on $ker\ \overline{h}$ as for any $ra + sb \in ker\ \overline{h}$, $a, b \in ker\ \overline{h}$, $r, s \in R$, we may select a representative $r\widetilde{a} + s\widetilde{b} \in B$ in its preimage, and the rest of the maps are compositions of homomorphisms and so respect the module structure on B. Thus, we have a well defined homomorphism $\delta : ker\ \overline{h} \to ker\ \overline{f}'$ via $a \mapsto \pi_\alpha(f'^{-1}(\beta(\widetilde{a})))$.

Now we claim that the following sequence is exact, where as above the left inclusion is induced by the first isomorphism theorem.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & im\ \overline{g} & \dashrightarrow & ker\ \overline{h} & \xrightarrow{\delta} & ker\ \overline{f} & \longrightarrow & 0 \\ & & \uparrow & \nearrow_{\overline{g}} & & & & & \\ & & ker\ \beta & & & & & & \end{array}$$

Let $\xi \in im\ \overline{g}$. We may choose a lift $\widetilde{\xi} \in ker\ \beta \subset B$ in the preimage $g^{-1}(ker\ \gamma)$, which we earlier showed can be used in the map without altering well-definedness of δ. We have that $\pi_\alpha(f'^{-1}(\beta(\widetilde{\xi}))) = \pi_\alpha(f'^{-1}(0)) = 0$ and so $\xi \in ker\ \delta$.

Now conversely let $\zeta \in ker\ \delta$. We have that $\pi_\alpha(f'^{-1}(\beta(\widetilde{\zeta}))) = 0 \implies f'^{-1}(\beta(\widetilde{\zeta})) \in im\ \alpha$. This implies, in particular, that $\beta(\widetilde{\zeta}) \in f'(im\ \alpha) = \beta(im\ f) \implies \widetilde{\zeta} \in im\ f + ker\ \beta \implies \zeta = g(\widetilde{\zeta}) \in g(ker\ \beta + im\ f) = im\ \overline{g}$ and so we have exactness in the middle.

The last order is to show that δ is surjective. Suppose $u \in ker\ \overline{f}'$. Let $\mu \in A'$ be a representative in the π_α-preimage of u. We have that $f'(\mu) \in \beta(B)$ as $\overline{f}' \circ \pi_\alpha(\mu) = 0 = \pi_\beta \circ f'(\mu)$. Let $\widetilde{\mu}_\beta \in B$ be a representative in the β-preimage of $f'(\mu)$. We have that $\gamma \circ g(\widetilde{\mu}_b) = g' \circ \beta(\widetilde{\mu}_\beta) = g' \circ f(\mu) = 0 \implies g(\widetilde{\mu}_\beta) \in ker\ \gamma$. Thus, $u = \pi_\alpha(f'^{-1}(\beta(\widetilde{\mu}_\beta))) = \delta(g(\mu_\beta))$ by definition $\implies \delta$ is surjective. Thus,

$$0 \longrightarrow im\ \overline{g} \hookrightarrow ker\ \overline{h} \xrightarrow{\delta} ker\ \overline{f} \longrightarrow 0$$

is exact, yielding the result. □

Problem 3

Let R be a Noetherian commutative ring, $\mathfrak{p}$ a prime ideal of R, and A and B finitely generated R-modules with $s \geq 0$.

a) **WTS** $\mathrm{Tor}_i^R(A,B)_\mathfrak{p} \cong \mathrm{Tor}_i^{R_\mathfrak{p}}(A_\mathfrak{p}, B_\mathfrak{p})$ and similarly for $\mathrm{Ext}_i^R(A,B)_\mathfrak{p}$.

Proof. We prove first the case for the Tor functor. Fix a projective resolution of A and apply the functor $- \otimes_R B$ to the truncation as below:

$$\ldots \longrightarrow P_3 \otimes_R B \longrightarrow P_2 \otimes_R B \longrightarrow P_1 \otimes_R B \longrightarrow P_0 \otimes_R B \longrightarrow 0$$

Note that extension of scalars to the localization $R_\mathfrak{p} \otimes_R -$ is a flat morphism. From Assignment 5, problem 1, we have that given additive functors G, L, with G exact, $L_i(G \circ F) \cong G \circ L_i F$ in the functor category. This yields that $R_\mathfrak{p} \otimes_R L_i(t_B(A)) = L_i(R_\mathfrak{p} \otimes_R t_B(A))$. We claim that the composition $R_\mathfrak{p} \otimes_R (- \otimes_R B)$ is naturally isomorphic to the functor $(R_\mathfrak{p} \otimes_R -) \otimes_{R_\mathfrak{p}} (R_\mathfrak{p} \otimes_R B)$ for finitely generated modules. By the fact that the ring is noetherian, we may select any projective resolution to be a resolution of finitely generated free modules by extending a finite presentation, and so the isomorphism will still respect left derivations on finitely generated modules. Consider the following finite presentation for A (this is possible as the ring is noetherian):

$$R^m \to R^n \to A \to 0$$

Applying the composition $R_\mathfrak{p} \otimes_R (- \otimes_R B)$ to the above, right exactness yields the exact sequence:

$$R_\mathfrak{p} \otimes_R (R^m \otimes_R B) \to R_\mathfrak{p} \otimes_R (R^n \otimes_R B) \to R_\mathfrak{p} \otimes_R (A \otimes_R B) \to 0$$

As tensor products commute with coproducts, we have that $R_\mathfrak{p} \otimes_R (R^m \otimes_R B) \cong (R_\mathfrak{p} \otimes_R (R \otimes_R B))^m \cong (R_\mathfrak{p} \otimes_R B)^m \cong (R_\mathfrak{p}^m \otimes_{R_\mathfrak{p}} (R_\mathfrak{p} \otimes_R B)) \cong (R_\mathfrak{p} \otimes_r R^m) \otimes_{R_\mathfrak{p}} (R_\mathfrak{p} \otimes_R B)$. This yields morphisms as below:

$$\begin{array}{ccccccc}
R_\mathfrak{p} \otimes_R (R^m \otimes_R B) & \longrightarrow & R_\mathfrak{p} \otimes_R (R^n \otimes_R B) & \longrightarrow & R_\mathfrak{p} \otimes_R (A \otimes_R B) & \longrightarrow & 0 \\
\downarrow \cong & & \downarrow \cong & & \vdots \alpha & & \\
(R_\mathfrak{p} \otimes_r R^m) \otimes_{R_\mathfrak{p}} (R_\mathfrak{p} \otimes_R B) & \longrightarrow & (R_\mathfrak{p} \otimes_r R^n) \otimes_{R_\mathfrak{p}} (R_\mathfrak{p} \otimes_R B) & \longrightarrow & (R_\mathfrak{p} \otimes_r A) \otimes_{R_\mathfrak{p}} (R_\mathfrak{p} \otimes_R B) & \longrightarrow & 0
\end{array}$$

And the dotted map α is a natural isomorphism induced by the universal property of the cokernel. We thus have the claim as above, which indicates that for finitely generated modules we have the chain of isomorphisms $\mathrm{Tor}_i^R(A,B)_\mathfrak{p} = R_\mathfrak{p} \otimes_R L_i(t_B(A)) \cong L_i(R_\mathfrak{p} \otimes_R t_B(A)) \cong L_i((R_\mathfrak{p} \otimes_r A) \otimes_{R_\mathfrak{p}} (R_\mathfrak{p} \otimes_R B)) = L_i(A_\mathfrak{p} \otimes_{R_\mathfrak{p}} B_\mathfrak{p}) = \mathrm{Tor}_i^{R_\mathfrak{p}}(A_\mathfrak{p}, B_\mathfrak{p})$ and we have thusly proved the claim for Tor.
From problem 7 of homework 4 of winter quarter, we have that $R_\mathfrak{p} \otimes_R \mathrm{Hom}_R(A,B) \cong \mathrm{Hom}_{R_p}(A_\mathfrak{p}, B_\mathfrak{p})$ for finitely presented modules (here equivalent to finitely generated). Thus, using the same isomorphism and logic as above for finitely generated modules yielding finitely generated resolutions, we have $R_\mathfrak{p} \otimes_R L_i\mathrm{Hom}_R(A,B) \cong L_i(R_\mathfrak{p} \otimes_R \mathrm{Hom}_R(A,B)) \cong L_i\mathrm{Hom}_{R_p}(A_\mathfrak{p}, B_\mathfrak{p})$ which is the result. □

b) **WTS** Show that the annihilator of A has height at least s if and only if $A_\mathfrak{p} = 0$ for every prime of height less than s.

Proof. Suppose the annihilator of A has height s. Then in particular no prime ideal of height less than s contains $ann(A)$, and so for all primes $\mathfrak{p}$ of height less than s, $R - \mathfrak{p} = S_\mathfrak{p} \cap ann(A) \neq \emptyset$. Thus, $S_\mathfrak{p}^{-1}A = 0$ as some element in the annihilator must act invertibly on $S^{-1}A$. Now suppose $A_\mathfrak{p} = 0$ for every prime of height less than s. Then in particular no prime of height less than s contains $ann(A)$ as otherwise $(A/ann(A))_\mathfrak{p}$ would be nonzero and $A_\mathfrak{p} \twoheadrightarrow (A/ann(A))_\mathfrak{p}$ is still a surjection implying the codomain is nonzero, a contradiction. Thus, $ann(A)$ can only be contained in a prime of height greater than s and we have the result. □

c) **WTS** Two distinct proofs that $ann(A)$ has height $s \implies \operatorname{Tor}_i^R(A,B)$ and $\operatorname{Ext}_i^R(A,B)$ have annihilators of height at least s.

Proof. From parts a) and b) we have that $\operatorname{Tor}_i^R(A,B)_\mathfrak{p} \cong \operatorname{Tor}_i^{R_\mathfrak{p}}(A_\mathfrak{p}, B_\mathfrak{p})$ and similarly for Ext; thus, if the annihilator of A has height at least s then $A_\mathfrak{p}$ is zero for all primes $\mathfrak{p}$ of height less then s, and so $A_\mathfrak{p} = 0 \implies \operatorname{Tor}_i^R(A,B)_\mathfrak{p} \cong \operatorname{Tor}_i^{R_\mathfrak{p}}(0, B_\mathfrak{p}) = 0$ for all primes of height less than s, and similarly for Ext, implying that $\operatorname{Tor}_i^R(A,B)$ and $\operatorname{Ext}_i^R(A,B)$ have annihilators of height at least s.

For the second proof, fix a projective resolution of A. We see that the multiplication map $s : A \to A$ via $a \mapsto sa$ extends to a morphism of projective resolutions:

$$\begin{array}{ccccccccccc} \ldots & \longrightarrow & P_3 & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & A \\ & & \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle s} \\ \ldots & \longrightarrow & P_3 & \longrightarrow & P_2 & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & A \end{array}$$

And upon application of the tensor product yields:

$$\begin{array}{ccccccccccc} \ldots & \longrightarrow & P_3 \otimes_R B & \longrightarrow & P_2 \otimes_R B & \longrightarrow & P_1 \otimes_R B & \longrightarrow & P_0 \otimes_R B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle s} & & \downarrow{\scriptstyle s} \\ \ldots & \longrightarrow & P_3 \otimes_R B & \longrightarrow & P_2 \otimes_R B & \longrightarrow & P_1 \otimes_R B & \longrightarrow & P_0 \otimes_R B & \longrightarrow & 0 \end{array}$$

And this induced lift of the map $s : A \to A$ must be a map unique up to chain homotopy by the fact that the resolution is projective and by properties of derived functors (proved in class). Now for $s \in ann(A)$, we have that the above map $s : A \to A$ must be the zero map, and thus we may extend it to both the multiplication by s map and the 0 map on projective resolutions. Upon application of the tensor product, this yields two maps given by multiplication by s and the 0 map. However, these maps must be the same up to chain homotopy equivalence: i.e. they induce the same map on homology, and in particular for any i the induced multiplication by s map $s : \operatorname{Tor}_i^R(A,B)$ must be the 0 map, and so $s \in ann(\operatorname{Tor}_i(A,B)$. In particular, $ann(A) \subseteq \operatorname{Tor}_i^R(A,B)$, implying that the annihilator must contain $ann(A)$, and so any prime containing the annihilator must contain $ann(A)$ and thus must be of height at least s, implying the annihilator is of height at least s. Symmetric logic applies for Ext, replacing the tensor product with the $\operatorname{Hom}_R(-,B)$ functor above. □

d) **WTS** A projective resolution for F as an $R = F[x,y,z]$.

Proof. Consider the following projective resolution:

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & R & \xrightarrow{\delta} & R^3 & \xrightarrow{A} & R^3 & \xrightarrow{(x,y,z)} & R \\ & & & & & & & & \downarrow{\scriptstyle \pi} \\ & & & & & & & & F \end{array}$$

Where $A = \begin{pmatrix} y & z & 0 \\ -x & 0 & -z \\ 0 & -x & y \end{pmatrix}$, and $\pi : R \to F$ is the canonical projection. This complex is clearly exact, as the kernel of (x,y,z) is generated by $(xe_2 - ye_1, xe_3 - ze_1, ye_3 - ze_2)$, and as two of the columns in A are linearly independent, the kernel of A is at most one dimensional over R and here is generated by $(ze_1 - ye_2 + xe_3)$. The map δ on the left represents this kernel given by $\begin{pmatrix} -z \\ y \\ x \end{pmatrix}$ □

e) **WTS** $\mathrm{Ext}_i^R(F,R)$ and $\mathrm{Tor}_i^R(F,F)$.

Proof. We first compute $\mathrm{Tor}_i^R(F,F)$. Tensoring the above complex with F, we get (noting the "Id" by right exactness):

$$0 \longrightarrow F \xrightarrow{0} F^3 \xrightarrow{0} F^3 \xrightarrow{0} F \xrightarrow{Id} F$$

Where all maps disappear as their images lie in $(x,y,z)P_i$ for the corresponding projective P_i. Thus, the resultant Tor values are

$$\mathrm{Tor}_i^R(F,F) \cong \begin{cases} F & i=0 \\ F^3 & i=1 \\ F^3 & i=2 \\ F & i=4 \\ 0 & i \geq 5 \end{cases}$$

Now, applying $\mathrm{Hom}_R(-,R)$ to the above complex and noting that $\mathrm{Hom}_R(R,R^m) \cong R^m$, we get:

$$0 \longleftarrow R \xleftarrow{\delta^*} R^3 \xleftarrow{A^T} R^3 \xleftarrow{\begin{pmatrix} x \\ y \\ z \end{pmatrix}} R \xleftarrow{} 0$$

Note firstly that $A^T = \begin{pmatrix} y & -x & 0 \\ z & 0 & -x \\ 0 & -z & y \end{pmatrix}$, the kernel of which is generated by (x,y,z), which is precisely the image of the previous coboundary map. Next, the map δ^* is given by the row vector $(-z,y,x)$. $ker\delta^*$ is generated by $(y,z,0),(x,0,z),(0,-x,y)$, which is precisely the image of A^T. Thus, all cocycles must be coboundaries, and we get that $\mathrm{Ext}_i^R(F,R) = 0 \ \forall i$. □

Problem 4

Consider the group

$$G = \mathbb{F}_2^3 \rtimes_\phi \Sigma_3$$

With $\Sigma_3 \hookrightarrow GL_3(\mathbb{F}_2)$ via the permutation representation.

a) **WTS** All the conjugacy classes and orders of G.

Proof. We represent elements in the subgroups $\mathbb{F}_2^3$ as vectors of the form (a,b,c), and elements of Σ_3 by their cycle type. This is also understood to be the notation throughout this problem. Using the semidirect product structure and fact that $\mathbb{F}_2^3 \cdot \Sigma_3 = G$ so all elements are of the form of this product, we may compute all possible conjugacy classes directly by conjugating by all elements of the form $r\sigma$ for $r \in \mathbb{F}_2^3, \sigma \in \Sigma_3$. The

table of them is shown below:

Conjugacy class	Members of class	Order
(0,0,0) = 1	{1}	1
(1,0,0)	{(1,0,0), (0,1,0), (0,0,1)}	3
(0,1,1)	{0,1,1), (1,0,1), (1,1,0)}	3
(1,1,1)	{(1,1,1)}	1
(123)	{(123), (1,1,0)(123), (1,0,1)(123), (0,1,1)(123), (132), (1,1,0)(132), (1,0,1)(132), (0,1,1)(132)}	8
(12)	{(12), (23), (31), (1,1,0)(12), (1,0,1)(13), (0,1,1)(23)}	6
(1,0,0)(12)	{(1,0,0)(12), (0,1,0)(12), (0,1,0)(23), (0,0,1)(23), (1,0,0)(31), (0,0,1)(31)}	6
(0,0,1)(12)	{(0,0,1)(12), (1,0,0)(23), (0,1,0)(31), (1,1,1)(12), (1,1,1)(31), (1,1,1)(23)}	6
(0,1,1)(12)	{(0,1,1)(12), (1,0,1)(12), (1,1,0)(23), (1,0,1)(23), (0,1,1)(31), (1,1,0)(31)}	6
(1,0,0)(123)	{(1,0,0)(123), (0,1,0)(123), (0,0,1)(123), (1,1,1)(123) (1,0,0)(132), (0,1,0)(132), (0,0,1)(132), (1,1,1)(132)}	8

□

b) **WTS** Irreducible complex abelian representations of G.

Proof. We have that $(1,1,0) = (1,0,0)(12)(1,0,0)(12) \in [G,G]$, and similarly for $(0,1,1)$. Note that $H =< (1,1,0),(0,1,1) >$ is a normal subgroup of order 4: for any $\sigma \in \Sigma_3$, $\sigma(0,1,1)\sigma^{-1} \in \{(0,1,1),(1,0,1),(1,1,0)\}$ and so for any $k \in \mathbb{F}_2^3$, $k\sigma(1,1,0)\sigma^{-1}k^{-1} \in H$. Thus, $G/[G,G]$ is a quotient of $G/H = (\mathbb{F}_2^3/H) \rtimes_\phi \Sigma_3 = \mathbb{F}_2 \times \Sigma_3$ (no semidirect products over $\mathbb{F}_2$ as no nontrivial automorphisms). We know that the derived subgroup of the above group is $\mathbb{F}_2 \times [\Sigma_3, \Sigma_3]$, and thus the minimal abelian quotient of G given by $G/[G,G] = (G/H)/([\Sigma_3,\Sigma_3] = \mathbb{F}_2 \times \mathbb{F}_2$. Thus, any complex abelian representation of G is given by a homomorphism $\mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{C}^\times$: $\mathrm{Hom}(\mathbb{F}_2^2, \mathbb{C}^\times) = \mathrm{Hom}(\mathbb{F}_2, \mathbb{C}^\times)^2$ where $\mathrm{Hom}(\mathbb{F}_2, \mathbb{C}^\times)$ either sends $\overline{1} \to -1$ or to 1. This yields four distinct abelian representations, namely the trivial representation, the sign character on Σ_3 sending the conjugacy class of (12) to -1, the sign character on $\mathbb{F}_2^3$ sending $(1,0,0)$ to -1, and the product of both in $\mathbb{C}^\times$. □

c) **WTS** An irreducible 2-dimensional representation of G.

Proof. We have the natural surjection $G \twoheadrightarrow \Sigma_3 \cong D_6$ via the semidirect product structure. We know that $D_6 = < s, r \mid srs = r^{-1},\ s^2 = e,\ r^3 = e >$ has 3 conjugacy classes, namely $\{e\}, \{r, r^2\}, \{s.rs, r^2 s\}$. These correspond to the trivial representation, the sign representation $D_6 \twoheadrightarrow \mathbb{F}_2 \hookrightarrow \mathbb{C}^\times$, and an irreducible two dimensional representation (as $1 + 1 + n^2 = |D_6| = 6 \implies n = 2$. This two dimensional representation can be viewed as a quotient of the standard permutation representation on
bC^3 as follows: we have the injective permutation map $\Sigma_3 \hookrightarrow GL_3\mathbb{C}$ by permuting the basis elements. This $\mathbb{C}[G]$ module structure has a G-invariant subspace spanned by the diagonal element $(1,1,1) \in \mathbb{C}^3$. By semisimplicity, this must correspond to a trivial representation summand $\mathbb{C}$, as it is an irreducible submodule. Quotienting by this one dimensional summand, we get a two dimensional representation $\mathbb{C}^2$, and this map is injective by viewing the standard permutation map $\Sigma_3 \hookrightarrow GL_3(\mathbb{C})$ in a basis containing $(1,1,1)$ as the first element and looking at the bottom left two-dimensional block. As this map is injective, not every element in the image of this map can be simultaneously diagonalized as there are at least two noncommuting elements, r and s. Thus, the representation is not a direct sum of two trivial representations and thus must be irreducible. □

d) **WTS** G has a quotient of order 24 that is isomorphic to Σ_4.

Proof. Consider the cycles $\sigma = (13)(24), \tau = (14)(32) \in \Sigma_4$. We have that they are both distinct elements of order 2, and that $\sigma\tau = \tau\sigma = (14)(23)$. Thus, the group $< \sigma, \tau > \cong \mathbb{F}_2^2$. Consider the group $< (12), (123) > \cong \Sigma_3 \hookrightarrow \Sigma_4$. We have that $\Sigma_3 \cap < \sigma, \tau > = \{1\}$. Furthermore, note that $(123)(12)(34)(132) = (23)(14)$, $(123)(13)(24)(132) = (23)(14)$, $(12)(12)(34)(12) = (12)(34)$, $(12)(13)(24)(12) = (14)(23)$, $(12)(14)(23)(12) = (24)(13)$. Thus, as the generators normalize $\mathbb{F}_2^2$ the entire subgroup Σ_3 must normalize $\mathbb{F}_2^2$ and thus $\mathbb{F}_2^2 \cdot \Sigma_3 = \Sigma_3$ (as the degree of this subgroup is $24 = |\Sigma_4|$) can be written as a semidirect product $\Sigma_4 \cong \mathbb{F}_2^2 \rtimes_\phi \Sigma_3$ where from above it is evident that Σ_3 acts by permutations on the set $\{(1,0),(0,1),(1,1)\}$. Note that in our group G, we have an element in the center given by $(1,1,1) \in \mathbb{G}$, as all permutations fix it and it commutes with every element in $\mathbb{F}_2^3$. Thus, $< (1,1,1) >:= N \triangleleft G$, and we have that G/N is the group $\mathbb{F}_2^3/N \rtimes_\phi \Sigma_3$ where Σ_3 acts on $\mathbb{F}_2^3/N$ by permuting the representatives $\overline{(1,0,0)}, \overline{(0,1,0)}, \overline{(0,0,1)}$ in $\mathbb{F}_2^3/N$. However, $(0,0,1) \equiv (1,0,0) + (0,1,0) \mod (1,1,1)$ and so Σ_3 acts by permutations on the set $\{\overline{(1,0,0)}, \overline{(0,1,0)}, \overline{(1,0,0)} + \overline{(0,1,0)},\}$ which can be rewritten as $\mathbb{F}_2^2 \rtimes_\phi \Sigma_3$ where $\overline{(1,0,0)}, \overline{(0,1,0)}$ generate the summands on the left and Σ_3 acts by permuting $(1,0),(0,1),(1,1) \in \mathbb{F}_2^2$. As this is the same presentation as above, $G/N \cong \Sigma_4$. □

e) **WTS** If χ is an irreducible character and ψ is an abelian character then $\chi\psi$ is an irreducible character.

Proof. It suffices to show that for an irreducible representation V, the tensor product $W = V \otimes_{\mathbb{C}} \mathbb{C}$ for $\mathbb{C}$ an abelian representation corresponding to ψ, as the character of the above representation is $\chi\psi$. Let $v \otimes z \in W$ arbitrary. As V is irreducible, $\exists l = \sum_{i=1}^{|G|} c_i g_i$ with $c_i \in \mathbb{C}, g_i \in G$ s.t. $l(v) = 1$. Thus, $l(v \otimes z) = l(v) \otimes l(z) = 1 \otimes l(v)$ and as $l(z) \in \mathbb{C}$ we have that $\frac{l}{l(z)}(v \otimes z) = (1 \otimes 1)$. Thus, as $V \otimes \mathbb{C}$ is cyclic (i.e. generated by one element) over $\mathbb{C}[G]$ we have that it must be an irreducible $\mathbb{C}[G]$ module and thus we have the claim. □

f) **WTS** The character table of G.

Proof. We have that Σ_4 is a quotient of G by $< (1,1,1) >$ and so the character table of Σ_4 lies in the character table of G. As Σ_4 has 5 conjugacy classes, there are 5 irreducible representations. By the lemma above, tensoring with an abelian representation yields another irreducible representation, so we may tensor with the sign permutation ψ sending $(1,0,0) \mod < (0,1,1),(1,0,1) >$ to -1, yielding 10 distinct representations, which correspond to 10 different conjugacy classes. Consider thus following table, where the upper half entries are the representations coming from Σ_4 and the lower half are obtained by tensoring with the sign permutation just mentioned. Note that the conjugacy classes of Σ_4 can easily be determined down below using the isomorphism defined above, where $[(1,0,0) \mod (1,1,1)] \mapsto (13)(24), [(0,1,0) \mod (1,1,1)] \mapsto (14)(23), [(0,0,1) \mod (1,1,1)] \mapsto (12)(34)$.

	1	(1,0,0)	(0,1,1)	(1,1,1)	(123)	(12)	(1,0,0)(12)	(0,0,1)(12)	(1,0,0)(123)	(0,1,1)(12)
χ_{triv}	1	1	1	1	1	1	1	1	1	1
χ_{sgn}	1	1	1	1	1	-1	-1	-1	1	-1
χ_3	2	2	2	2	-1	0	0	0	-1	0
χ_σ	3	-1	-1	3	0	1	-1	1	0	-1
$\chi_\sigma\chi_{\text{sgn}}$	3	-1	-1	3	0	-1	1	-1	0	1
χ_ψ	1	-1	1	-1	1	1	-1	-1	-1	1
$\chi_{\text{sgn}}\chi_\psi$	1	-1	1	-1	1	-1	1	1	-1	-1
$\chi_3\chi_\psi$	2	-2	2	-2	-1	0	0	0	1	0
$\chi_\sigma\chi_\psi$	3	1	-1	-3	0	1	1	-1	0	-1
$\chi_\sigma\chi_{\text{sgn}}\chi_\psi$	3	1	-1	-3	0	-1	-1	1	0	1

□

Problem 5

For p an odd prime, let G be the group given by:

$$\mathbb{F}_p \rtimes_\varphi (\mathbb{F}_p)^\times$$

With $\varphi(a)(b) = ab$.

a) **WTS** G has $p-1$ complex abelian representations and one irreducible representation of dimension $p-1$.

Proof. During this proof, we use K to refer to $\mathbb{F}_p$, H to refer to $\mathbb{F}_p^\times$: i.e. $G \cong K \rtimes_\varphi H$. As G is a semidirect product, all elements can be written in the form $\sigma\tau$ for $\sigma \in K, \tau \in H$. First, we compute the conjugacy classes of G. We know that $\overline{b} \cdot \zeta \cdot \overline{a} \cdot \zeta^{-1} \cdot \overline{-b} = \overline{b + \zeta a - b} = \overline{\zeta a} \in K$ for $\overline{a}, \overline{b} \in K$, $\zeta \in H$. Thus, for $\overline{a} \neq \overline{0}$, we have that the conjugacy class $C_{\overline{a}} \supseteq \{\overline{a} \mid \overline{a} \in K^\times\}$ as the semidirect product over $\varphi : H \xrightarrow{\cong} Aut(K)$ means all generators of K, i.e. $K^\times$, are contained in the same conjugacy class under conjugation by H. Now let $\zeta \in H$. For $\overline{a} \in K$, $\zeta, \xi \in H$, we have that $\overline{a} \cdot \xi \cdot \zeta \cdot \xi^{-1} \cdot \overline{-a} = \overline{a} \cdot \zeta \cdot \overline{-a} = \overline{a - \zeta a} \cdot \zeta = \overline{(\zeta - 1)a} \cdot \zeta$. Thus, for all $\zeta \neq \overline{1} \in H$, the class $C_\zeta = \{\overline{(\zeta - 1)a} \cdot \zeta \mid a \in K\}$. Summarizing, we have:

$$G \supseteq \{e\} \cup \{K\} \setminus \{e\} \ \cup \bigcup_{\zeta \in H \setminus \{e\}} \left(\{\overline{(\zeta - 1)a} \cdot \zeta \mid \overline{a} \in K^\times\} \cup \{\zeta\} \right)$$

Where e refers to the identity. As the sum of the cardinalities of the classes above is $1 + (p-1) + (p)(p-2) = p(p-1)$ we have that the above expression is an equality, and there are p distinct conjugacy classes.

We know that $G/(K) \cong (K)^\times$ is a cyclic group of order $p-1$. Thus, we may define a homomorphism $\psi : H \cong \mathbb{Z}/(p-1)\mathbb{Z} \to \mathbb{C}^\times$ via $\sigma \mapsto \zeta_{p-1}$ for σ a generator. As they are both abelian groups and in particular $\mathbb{Z}$-modules, we have that for $k \in \mathbb{Z}$, $k\varphi : \mathbb{Z}/(p-1)\mathbb{Z} \to \mathbb{C}^\times$ are all distinct homomorphisms for $k \in \{1, ..., p-1\}$, where $(p-1)\varphi$ is the trivial homomorphism. As $\mathbb{C}^\times \cong Aut_{\mathbb{C}}(\mathbb{C})$ as a vector space, this family of homomorphisms represents $p-1$ distinct abelian $\mathbb{C}[G]$-module structures on $\mathbb{C}$, corresponding to $p-1$ distinct complex abelian representations including the trivial one. As we have that $p(p-1) = \sum_1^p n_p^2 = p - 1 + n_p^2$ for n_i the dimensions of the irreducible representations, we have that the dimension $n_p = p-1$. Thus, there are $p-1$ complex abelian representations and one irreducible representation of dimension $p-1$. Note that this gives us a Wedderburn decomposition:

$$\mathbb{C}[G] \cong \mathbb{C} \times \mathbb{C}^{p-1} \times GL_{p-1}(\mathbb{C})$$

□

b) **WTS**: Artin-Wedderburn decomposition of $\mathbb{R}[G]$.

Proof. As above, we have a quotient of G given by $G/K = \mathbb{F}_p^\times \cong \mathbb{Z}/p\mathbb{Z}$. Thus, the Artin-Wedderburn decomposition for $\mathbb{R}[\mathbb{F}_p^\times]$ is part of the decomposition for G. We note that $\mathbb{R}[\mathbb{Z}/p\mathbb{Z}] \cong \mathbb{R}[t]/(t^{p-1} - 1)$ via t maps to the generator of $\mathbb{F}_p^\times$. We have that over $\mathbb{R}$, $t^{p-1} - 1 \cong (t-1)(t^{p-2} - t^{p-3} + ... - 1) = (t-1) \cdot \prod_{f_i \in A} f_i \cdot \prod_{g_j \in B} g_j$ for A the set of all degree 1 irreducible factors of $t^{p-2} - t + ... - 1$ and B the set of all degree 2 irreducible factors of the same. We thus have, by CRT,

$$\mathbb{R}[\mathbb{F}_p^\times] \cong \mathbb{R} \times \mathbb{R}^{|A|} \times \mathbb{C}^{|B|}$$

Which includes the trivial representation as the term corresponding to $\mathbb{R}/(t-1)$.

Now, consider the symmetric group Σ_p. Let $\sigma = (1234...p)$ be some p-cycle. Define $\kappa : \mathbb{F}_p \xrightarrow{\cong} < \sigma >$ via $1 \mapsto (123...p)$. Let a generate $\mathbb{F}_p^\times \cong Aut(\mathbb{F}_p)$ via the normal multiplication map. We note that $\kappa(a) =$

$(123...p)^a = (1[1+a][1+2a]...[1+(p-1)a])$ for $[x]$ the residue class represenative of $[x]$ in $\{1....p\}$. Consider the element τ defined by the permutation sending $n \to [1+(n-1)a]$. Note then that

$$\tau\sigma\tau^{-1} = \tau(123...p)\tau^{-1} = (1\tau(2)\tau(3)...\tau(p)) = (1[1+a][1+2a]...[1+(p-1)a]) = \sigma^a$$

We also note that for n minimal s.t. $\tau^n\sigma\tau^{-n} = \sigma$, we must have $\sigma^{a^n} = \sigma \iff a^n \equiv 1 \mod p \implies n = p-1$ by the fact that a generates $\mathbb{F}_p^\times$, and so τ must be a $(p-1)$-cycle. Thus, $< \sigma > \cap < \tau >= 1$, clearly $< \sigma > \triangleleft < \sigma, \tau >$ as for any n, m, $\sigma^m\tau^n\sigma\tau^{-n}\sigma^{-m} \in < \sigma >$, and so the subgroup $< \sigma, \tau >$ has a presentation as a semidirect product, given by $\varphi : \tau \to Aut(< \sigma >)$ via $\tau \mapsto (\sigma \mapsto \sigma^a)$. By choice, we may write $< \tau > \cong \mathbb{F}_p^\times$ by $\tau \mapsto a$, along with the same map $\kappa :< \sigma > \to \mathbb{F}_p$ and by construction, the semidirect product above may be written as $\mathbb{F}_p \rtimes_\varphi \mathbb{F}_p^\times$ via $\phi(a)(b) = a \cdot b$. Thus, the subgroup $< \sigma, \tau > \cong G$, and we have $G \hookrightarrow \Sigma_p$. This provides us a map $\psi : G \hookrightarrow GL_p(\mathbb{R})$ via the standard permutation representation of matrices, yielding an injective representation $\mathbb{R}[G] \circlearrowright \mathbb{R}^p$. Note that under the permutation representation, we have a one-dimensional G-invariant subspace corresponding to the diagonal element $(1, 1, ..., 1) \in \mathbb{R}^p$. We have that any G-invariant subspace of a representation is a direct summand corresponding to the trivial representation, by semisimplicity. Thus, we have that the representation above splits as a direct sum of modules:

$$\mathbb{R}[G] \circlearrowright \mathbb{R}^p = \mathbb{R}^{p-1} \oplus \text{span}\{(1, 1, ..., 1)\} = \mathbb{R}^{p-1} \oplus R[G]/(G)$$

Which gives us an injective map by restriction $\phi : G \to GL_{p-1}(\mathbb{R})$, and thus a map $\widetilde{\phi}_\mathbb{R} : R[G] \to M_{p-1}(R)$. Note that we also have $\widetilde{\phi} : \mathbb{C}[G] \hookrightarrow M_{p-1}(\mathbb{C})$ via the exact same map $\phi : G \to GL_{p-1}(\mathbb{R}) \hookrightarrow GL_{p-1}(\mathbb{C})$. Now that if this representation $\mathbb{C}[G] \circlearrowright {}_\phi\mathbb{C}^{p-1}$ splits at all, then it splits as a direct sum of 1-dimensional abelian representations due to the structure of the Wedderburn decomposition of $\mathbb{C}[G]$ above (only simple modules are dimension 1 or dimension p-1). However, if this were the case, then all operators in $im(G) \subset GL_{p-1}(\mathbb{C})$ under this representation would be simultaneously diagonalizable, due to acting diagonally on one dimensional subspaces. This however, is not true, as the injectivity of ϕ implies there exist $g_1, g_2 \in im(G)$ which do not commute with each other and thus cannot be simultaneously diagonalized (conjugation is an automorphism). Thus, this representation of $\mathbb{C}[G]$ is the unique irreducible representation of dimension $p-1$, implying that the map of $\mathbb{C}$-modules given by $\widetilde{\phi} : \mathbb{C}[G] \to M_n(\mathbb{C})$ is surjective, and so we may select $(p-1)^2$ $\mathbb{C}$-linearly independent elements $\{g_1, ..., g_{(p-1)^2}\} \subset im(G) \subset M_{p-1}(\mathbb{R}) \subset M_{p-1}(\mathbb{C})$ which form a basis for dimension reasons. This implies $\{g_1, ..., g_{(p-1)^2}\}$ form a linearly independent basis (again by dimension) for $M_{p-1}(\mathbb{R})$ over $\mathbb{R}$ under the map $\widetilde{\phi}_\mathbb{R} = \widetilde{\phi}_\mathbb{R}$. In particular, the map $\phi : G \to GL_{p-1}(\mathbb{R})$ must correspond to an irreducible representation as under this map $R[G] \circlearrowright \mathbb{R}^{p-1}$ transitively (by surjectivity of $\widetilde{\phi}_\mathbb{R}$), so $\mathbb{R}^{p-1}$ is generated by one element. Thus, our Artin-Wedderburn decomposition of $\mathbb{R}[G]$ so far contains the term $\mathbb{R} \times \mathbb{R}^{|A|} \times \mathbb{C}^{|B|} \times M_{p-1}(\mathbb{R})$, and as $1 + |A| + 2|B| = p - 1$ by degree reasons (sum of degrees of polynomials dividing $t^{p-1} - 1$), we have that the above decomposition is dimension $p - 1 + (p-1)^2 = p(p-1)$. Thus, our result is:

$$\mathbb{R}[G] \cong \mathbb{R} \times \mathbb{R}^{|A|} \times \mathbb{C}^{|B|} \times M_{p-1}(\mathbb{R})$$

For the case $p = 3$, the set $|A|$ of degree 1 irreducibles of $t - 1$ is just $\{t - 1\}$ and $|B|$ is empty, so the Wedderburn decomposition at 3 is

$$\mathbb{R}[G] \cong \mathbb{R} \times \mathbb{R} \times M_2(\mathbb{R})$$

At $p = 2$ the Wedderburn decomposition is trivially just $\mathbb{R}^2$. At higher primes, we have that the only $(p-1)$th roots of unity are 1 and -1, so $|A| = 1$ and the only remaining factors of $t^{p-2} - t^{p-3} + ... - 1$ must be degree two irreducible polynomials, so at higher primes the cardinality $|B| = (p-3)/2$. Putting this together, our general formula for the Wedderburn decomposition at a prime $p > 2$ is:

$$\mathbb{R}[G] \cong \mathbb{R} \times \mathbb{R} \times \mathbb{C}^{\frac{(p-3)}{2}} \times M_{p-1}(\mathbb{R})$$

□