MATH 122: HOMEWORK 3 SOLUTIONS

- Section 18.1 # 3,11,15,16,20
- Section 18.2 # 3

Let G be a finite group. The *commutator subgroup* G', also called the *derived subgroup* is the subgroup generated by all commutators $[x, y] = xyx^{-1}y^{-1}$. The word "generated by" is important since the product of commutators may not be a commutator. See Dummit and Foote Proposition 7 on page 169.

Section 18.1 #3. Prove that the degree 1 representations of G are in bijection with the degree 1 representations of G/G'.

Solution: We will use the following:

Lemma 1. *Let A be an abelian group. Then a homomorphism $\varphi : G \longrightarrow A$ contains G' in its kernel, hence factors through G/G'.*

Proof. Here "factors through" means that $\varphi = \Phi \circ p$ for some homomorphism $\Phi : G/G' \longrightarrow A$, where $p : G \longrightarrow G/G'$ is the projection map. To prove this, it is sufficient to show that G' is contained in the kernel of φ. To see that, note that $\varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1} = 1$, where we have used the fact that φ is a homomorphism and A is abelian. Since G' is the group generated by commutators $xyx^{-1}y^{-1}$, we see that $G' \subseteq \ker(\Phi)$. □

The Lemma means that there is a bijection between the homomorphisms $\varphi : G \longrightarrow A$ and $\Phi : G/G' \longrightarrow A$, in which $\varphi = \Phi \circ p$.

Now a degree 1 representation of G is a homomorphism $\pi : G \longrightarrow \mathrm{GL}(1, F) \cong F^\times$, which is abelian, so it factors through G/G'. So the problem is solved by taking $A = F^\times$.

Section 18.1 #11. Let $\varphi : S_n \to \mathrm{GL}_n(F)$ be the matrix representation given by the permutation module described in Example 3 in the second set of examples, where the matrices are computed with respect to the basis $e_1, \cdots, e_n$. Prove that $\det(\varphi(\sigma)) = \varepsilon(\sigma)$ for all $\sigma \in S_n$, where $\varepsilon(\sigma)$ is the sign of the permutation σ. [**Hint:** Check this on transpositions.]

Solution. Both $\varepsilon(\sigma)$ and $\det(\varphi(\sigma))$ are obviously homomorphisms $S_n \longrightarrow \mathbb{C}^\times$ and to prove they are equal, it is sufficient to show that they are the same when σ is an element of a generating set.

Lemma 2. *The group S_n is generated by $s_1, \cdots, s_{n-1}$ where $s_i = (i, i + 1)$.*

Proof. Step 1: S_n is generated by the $\frac{1}{2}n(n-1)$ transpositions (i, j) with $i < j$. Indeed, any permutation can be decomposed into a product of disjoint cycles, so it is enough to show that a cycle can be written as a product of transpositions and indeed:

$$(a_1, a_2, \cdots, a_r) = (a_1, a_2)(a_2, a_3)\cdots(a_{r-1}, a_r).$$

(Since $(i, j) = (j, i)$ it doesn't matter whether $a_i < a_{i+1}$ or $a_i > a_{i+1}$.)

Step 2: every transposition (i,j) with $i<j$ can be written as a product of s_i. We can prove this by induction on $j-i$. Indeed if $j-i>1$ then

$$(i,j)=(i+1,j)(i,i+1)(i+1,j)=(i+1,j)s_i(i+1,j)$$

and by induction $(i+1,j)$ can be written as a product of the s_i. □

These particular generators s_i of S_n are called *simple reflections* and are very important in representation theory.

We may now finish the solution of the problem. Let I_k be the $k\times k$ identity matrix.

$$\varphi(s_i)=\begin{pmatrix} I_{i-1} & 0 & 0 \\ 0 & \boxed{\begin{matrix}0 & 1\\ 1 & 0\end{matrix}} & 0 \\ 0 & 0 & I_{n-i-1}\end{pmatrix}, \qquad \det(\varphi(s_i))=\det\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}=-1,$$

so $\det(\varphi(s_i))=-1=\varepsilon(s_i)$. Since the homomorphisms $\det(\varphi(w))$ and $\varepsilon(w)$ agree on a set of generators they are the same.

Section 18.1 #15. Exhibit all 1-dimensional complex representations of a finite cyclic group; make sure to decide which are inequivalent.

Solution: Let $G=Z_n=\langle x|x^n=1\rangle$. A 1-dimensional representation of G is just a homomorphism $\pi: G\longrightarrow \mathrm{GL}(1,\mathbb{C})\cong\mathbb{C}^\times$. Since $x^n=1$, $\pi(x^n)$ must be an n-th root of unity ζ^k where $\zeta=e^{2\pi i/n}$. Conversely, given an n-th root of unity $\zeta^k=e^{2\pi ik/n}$ there is a one-dimensional representation

$$\pi_k(x^a)=(e^{2\pi ika/n}).$$

This gives us n distinct irreducible one-dimensional representations of Z_n.

Section 18.1 #16. Exhibit all 1-dimensional complex representations of a finite abelian group; deduce that the number of inequivalent degree 1 complex representations of a finite abelian group equals the order of the group. [First decompose the abelian group into a direct product of cyclic groups, then use the preceding exercise.]

Solution. It is useful to note that if G is a group and A is an abelian group, then $\mathrm{Hom}(G,A)$ is a group with pointwise multiplication: $(\chi_1\chi_2)(g)=\chi_1(g)\chi_2(g)$. Using this fact, we may upgrade the result of the last exercise: If $G=\langle z|z^n\rangle=1$ is cyclic, then by the previous exercise $\mathrm{Hom}(G,\mathbb{C}^\times)$ is also a group and as a group it is cyclic, generated by χ_ζ where $\zeta=e^{2\pi i/n}$.

Now a finite abelian group is a direct product of abelian groups, by either Theorem 3 or Theorem 5 in Dummit and Foote Section 5.2. We can combine this with the following result:

Proposition 1. *Let G and H be groups and let A be an abelian group. Then*

$$\mathrm{Hom}(G\times H,A)\cong\mathrm{Hom}(G,A)\times\mathrm{Hom}(H,A).$$

In this isomorphism $\theta\in\mathrm{Hom}(G\times H,A)$ corresponds to (φ,ψ) with $\varphi\in\mathrm{Hom}(G,A)$ and $\psi\in\mathrm{Hom}(H,A)$, where

$$\theta(g,h)=\varphi(g)\psi(h).$$

Proof. If $\theta\in\mathrm{Hom}(G\times H,A)$ is given then composing θ with the injection $i:G\to G\times H$ defined by $i(g)=(g,1)$ gives a homomorphism $\varphi=\theta\circ i$ in $\mathrm{Hom}(G,A)$. Similarly let $j:H\to G\times H$ be the injection $j(h)=(1,h)$. Then $\psi=\theta\circ j$ is in $\mathrm{Hom}(H,A)$. Putting these together $\theta\mapsto(\varphi,\psi)$ is a homomorphism

$$\alpha:\mathrm{Hom}(G\times H,A)\to\mathrm{Hom}(G,A)\times\mathrm{Hom}(H,A). \qquad \alpha(\theta)=(\theta\circ i,\theta\circ j).$$

Conversely, let $\varphi \in \mathrm{Hom}(G, A)$ and $\psi \in \mathrm{Hom}(H, A)$ be given. Then we can define $\theta(g, h) = \varphi(g)\psi(h)$. The fact that A is abelian is used in showing that this θ is a homomorphism. Indeed,

$$\theta((g_1, h_1)(g_2, h_2)) = \theta(g_1 g_2, h_1 h_2) = \varphi(g_1 g_2)\psi(h_1 h_2) = \varphi(g_1)\varphi(g_2)\psi(h_1)\psi(h_2)$$

while

$$\theta(g_1, h_1)\theta(g_2, h_2) = \varphi(g_1)\psi(h_1)\,\varphi(g_2)\psi(h_2).$$

These are equal since $\varphi(g_2)$ and $\psi(h_1)$ commute. So $(\varphi, \psi) \mapsto \theta$ with this definition is a homomorphism

$$\beta : \mathrm{Hom}(G, A) \times \mathrm{Hom}(H, A) \longrightarrow \mathrm{Hom}(G \times H, A).$$

It is easy to see that α and β are inverse homomorphisms. For example

$$\beta\alpha(\theta)(g, h) = \beta(\theta \circ i, \theta \circ j)(g, h) = (\theta \circ i)(g) \cdot (\theta \circ j)(h) = \theta(g, 1)\theta(1, h) = \theta((g, 1)(1, h)) = \theta(g, h)$$

proving $\beta \circ \alpha = 1_{\mathrm{Hom}(G \times H, A)}$. ☐

This result extends to an arbitrary finite product $G_1 \times \cdots \times G_n$ of groups:

$$\mathrm{Hom}(G_1 \times \cdots \times G_n, A) = \prod_i \mathrm{Hom}(G_i, A).$$

Now if G is a finite abelian group, it is a direct product of cyclic groups, so (taking $A = \mathbb{C}^\times$). So

$$\mathrm{Hom}(Z_{m_1} \times \cdots \times Z_{m_r}) = \prod \mathrm{Hom}(Z_{m_i}, \mathbb{C}^*) \cong \prod Z_{m_i}.$$

Conclusion: if G is a finite abelian group then so is the group $\mathrm{Hom}(G, \mathbb{C}^\times)$. This "dual" group is actually isomorphic to G. In particular the number of 1-dimensional representations of G equals $|G|$.

Section 18.1 #20. Prove that the number of degree 1 complex representations of any finite group equals $[G : G']$, where G' is the commutator subgroup of G. [**Hint:** use Exercises 3 and 16.]

Solution: By Exercise 3, every 1-dimensional representation of G factors through G/G', so the number of 1-dimensional representations of G equals the number of one-dimensional representations of G/G'. But the one-dimensional representations of any abelian group A (such as G/G') equals the order of A by Exercise 16. Thus the number of one-dimensional representations of G/G' equals $|G/G'| = [G : G']$.

In the next problem, let me distinguish between central idempotents and minimal idempotents. An idempotent e in a ring R is an element that satisfies $e^2 = e$. It is *central* if $ex = xe$ for all $x \in R$. In this case, Re is a 2-sided ideal. An ideal is *minimal* if Re is a simple left ideal. In Wedderburn's theorem, we decompose a semisimple ring R as a direct sum of two-sided ideals R_i each of which is the form Re_i where e_i is a central idempotent. Then R_i is itself a ring with unit e_i, and it further turns out that $R_i = \mathrm{Mat}_{d_i}(D_i)$ where D_i is a division ring. Now e_i itself can be further decomposed as a sum of minimal idempotents. To see this, let's consider the case where $R = \mathrm{Mat}_n(D)$ with D a division ring. Then we can write

$$1_R = e_1 + \ldots + e_n$$

where

$$e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$$

where the 1 is in the i-th column. The e_i are minimal idempotents, since Re_i consists of all matrices whose nonzero entries are in the i-th column, a module $\cong D^n$, which is a simple module. Note that the minimal idempotents are not central! For semisimple rings, the central idempotents can be further decomposed into minimal idempotents, as this example of $R = \mathrm{Mat}_n(D)$ shows. (For this ring, the only central idempotent is the identity matrix.)

Section 18.2 #3. Prove that (4) implies (3) in Wedderburn's Theorem. [**Hint:** Let N be a nonzero R-module. First show that N contains simple submodules by considering a cyclic submodule. Then use Zorn's Lemma applied to the set of direct sums of simple submodules (appropriately ordered) to show that N contains a maximal completely reducible submodule M. If $M \neq N$ let M_1 be teh complete preimage in N of a simple module in N/M and contradict the maximality of M.]

Solution. In (4), we are assuming that $R = L_1 \oplus \cdots \oplus L_n$ where the L_i are simple left ideals, $L_i = Re_i$ where $e_i^2 = e_i$ and $e_i e_j = 0$ if $i \neq j$ with $\sum e_i = 1$.

Let M be an R-module. We want to prove that M is a direct sum of irreducible modules. Thus we want to find a family M_i ($i \in I$) of simple (irreducible) submodules such that

$$M = \bigoplus_{i \in I} M_i.$$

(The indexing set I could be infinite.) This means that any element of m can be written *uniquely* as

$$m = \sum_{i \in I} m_i, \qquad m_i \in M_i$$

where $m_i = 0$ for all but finitely many i.

This will be proved by a Zorn's Lemma argument. Let Σ be the set of indexed families of submodules $\{M_i | i \in I\}$ such that the sum $\sum_i M_i$ is direct and M_i is simple (irreducible). More precisely, an element of Σ is an ordered pair $(I, \{M_i\})$ where I is an indexing set and for each $i \in I$ we are given a submodule M_i that is simple, and it is assumed that the sum

$$\sum_{i \in I} M_i$$

is direct. This assumption means that if

$$0 = \sum_{i \in I} m_i$$

with $m_i \in M_i$ and all but finitely many m_i zero, then all m_i are zero.

We order Σ by inclusion. More precisely we define

$$(I, \{M_i\}) \leqslant (J, \{N_k\}) \qquad \text{if} \qquad I \subseteq J \text{ and } M_i = N_i \text{ for } i \in I. \tag{1}$$

This is a *partial order*.

We will show that Σ has a maximal element. We will apply Zorn's Lemma, which is formulated in Appendix I in Dummit and Foote (page 908). To apply Zorn's Lemma, we have to prove that every totally ordered subset Θ of Σ has an upper bound. Here Θ being totally ordered means that if $(I, \{M_i\})$ and $(J, \{M_j\})$ are in Θ then either $(I, \{M_i\}) \leqslant (J, \{N_j\})$ or $(J, \{N_j\}) \leqslant (I, \{M_i\})$. Define K to be the union of I with $(I, \{M_i\}) \in \Theta$. If $k \in K$ then there exists some $(I, \{M_i\}) \in \Theta$ such that $k \in I$ and we define $M_k = M_i$. Note that by the definition (1) of the partial order $\leqslant$ this is well defined, independent of the choice of $(I, \{M_i\})$. This is because if $k \in J$ with $(J, \{N_j\}) \in \Theta$ then (1) guarantees that $M_k = N_k$. It is easy to see that $(K, \{M_k\}) \in \Sigma$ and this element dominates Θ. It is an upper bound for Θ.

Also Σ is nonempty since the "empty" family $(\varnothing, \{\ \}) \in \Sigma$.

Zorn's Lemma applies to imply that Σ has a maximal element. So let $(I, \{M_i\})$ be a maximal element of Σ.

We will prove that $M = \bigoplus_{i \in I} M_i$. The sum $\sum_{i \in I} M_i$ is direct, so we may denote this submodule

$$M_0 = \bigoplus_{i \in I} M_i$$

and the problem is to show that $M_0 \in M$. If not, let $x \in M - M_0$. We can write

$$x = \sum_{j=1}^{n} e_j x, \qquad e_j x \in L_j x.$$

Since $x \notin M_0$, we have $e_i x \notin M_0$ for some i. In particular $e_i x \neq 0$.

Lemma 3. *The left module $L_i x$ is simple (irreducible) and $L_i x \cap M_0 = 0$.*

Proof. Indeed we have a module homomorphism $\varphi : L_i \to L_i x$ defined by $\varphi(r) = rx$. Since L_i is simple, the image $\varphi_i(L_i) = L_i x$ is either simple or zero. But it is nonzero since it contains $e_i x$. Now $L_i x \cap M_0$ is either $L_i x$ or 0. Since $e_i x \notin M_0$ we get $L_i x \cap M_0 = 0$. □

The Lemma implies that the sum $L_i x + M_0$ is direct. So we can enlarge the family $(I, \{M_i\})$ by adding a new index $j \notin I$ with $M_j = L_i x$. Then $(I \cup \{j\}, \{M_i\}) \in \Sigma$ is strictly greater than $(I, \{M_i\})$, contradicting the maximality of $(I, \{M_i\})$. This contradiction proves that $M_0 = M$ and we are done.