Math 6000, Fall 2020 (Prof. Kinser), Homework 7

Nitesh Mathur

3 November 2020

Source Discussed problem/solutions with Zach Bryhtan.

Problem 1. *Skills developed: connecting representations of related groups.* Let G be any group (not necessarily finite) and $G' = [G, G]$,the commutator subgroup of G. Explicitly describe (with justification) a bijection between the sets of one-dimensional representations of G and of the abelianization G/G'.

Defs/Thms Let G be a group.

1. A **linear representation** of G is a homomorphism $G \to GL(V)$ for some vector space V.
2. A **matrix representation** of G is a homomorphism $G \to GL_n(F)$.
3. (Example 5 in class) Given a field F and group homomorphism $G \to F^\times = GL_1(F)$, we get a 1 dimensional representation of G.
4. G/G' is the largest abelian quotient of G, where G' is the commutator subgroup.

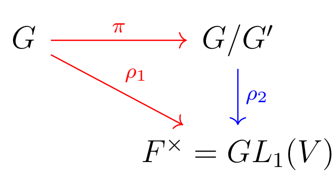
Proof Let F be a field.

Let $\rho_1 : G \to F^\times = GL_1(F)$ and $\rho_2 : G/G' \to F^\times = GL_1(F)$ be one-dimensional representations of G and G/G' respectively (by example 5).

Consider the natural projection map $\pi : G \to G/G'$ defined by $\pi(g) = gG'$ for $g \in G$.

Now, we need to show that $\varphi : \rho_1 \to \rho_2$ is a bijection.

Then, we have the following maps:



By the universal property, we have a unique map $\rho_1 = \rho_2 \circ \pi : G \to GL_1(V)$. Hence, the correspondence between ρ_1 and ρ_2 is bijective.

$\therefore$, there is a bijection between the sets of one-dimensional representation of G and the abelianization G/G'.

Problem 2. *Skills developed: understanding a fundamental property of simple modules.*

Let R be a ring and M, N be simple left R-modules. Prove that any nonzero homomorphism from M to N is an isomorphism. Conclude that $\text{End}_R(M)$ is a division ring.

Proof. (a) Let $\phi : M \to N$ be an R-module homomorphism such that ϕ is nonzero.

By the First Isomorphism Theorem (of Modules), $\ker(\phi) \leq M$ and $M/\ker(\phi) \cong \phi(M)$.

Since M is simple, the only submodules of M are 0 and M itself. Hence, $\ker(\phi) = 0$ or $\ker(\phi) = M$.

Because $\phi \neq 0, \ker(\phi) = 0$.

Therefore, we have $M/\ker(\phi) \cong M/\{0\} \cong M \cong \phi(M) = N$.

(since the image of ϕ is a nonzero submodule of N, which is also simple).

Hence, $M \cong N$ and ϕ is an isomorphism.

(b) From the notation above, suppose $N = M$ also. Then, we have $\phi : M \to M$, i.e. $\phi \in \text{End}_R(M)$.

In part (a), we proved that ϕ is an isomorphism. In particular, it has a two-sided inverse.

$\therefore$, $\text{End}_R(M)$ is a division ring.

Extra (From Wikipedia) Part (b) in general is known as the Schur's Lemma stated below:

Let V and W be vector space with underlying field $\mathbb{C}$. Let ρ_V and ρ_W be irreducible representations of G on V and W respectively. Then,

(i) V and W not isomorphic, then there are no non-trivial G-linear maps between them.

(ii) If $V = W$ and if $\rho_V = \rho_W$, then the only non-trivial maps are the identity and scalar multiples of identity.

If R is an algebra, $M = N$ is a simple module, then by Schur's Lemma, the endomorphism ring of M is a division algebra over a field k.

(Also, Chapter 18, Lemma 7).

Problem 3. *Skills developed: working with group rings and short exact sequences, and familiarity with fundamental "issue" of modular representation theory of groups (i.e. in positive characteristic.)*

We will later study *semisimple* rings, which can be characterized as having every module both projective and injective, or equivalently every short exact sequence of modules over that ring splits. Let G be a group and K a field of characteristic $p > 0$. The goal of this problem is to prove that the group ring KG is *not* semisimple if p divides $|G|$. (We will prove the converse in class, call Maschke's theorem, so the statement above is "if and only if".)

Since $\{g \in G\}$ is a basis of KG, the *augmentation map*

$$\epsilon : KG \to K, \quad \epsilon(\sum_{g \in G} a_g g) = \sum_{g \in G} a_g$$

is well-defined. Let $I := \ker(\epsilon)$. Recall that K can be regarded as a KG-module by the action $g.x = x$ for all $x \in K$, called the *trivial* KG-module.

(a) Prove that ϵ is a morphism of KG-modules, and a ring homomorphism. Conlcude that I is a 2-sided ideal of KG.

(b) Consider the short exact sequence of KG- modules

$$0 \to I \to KG \xrightarrow{\epsilon} K \to 0.$$

If KG were to be a semi-simple ring, then ϵ would necessarily split, giving a decomposition $KG \cong I \oplus J$ as KG-modules where $J \subset KG$ is a trivial KG-module. Let $v = \sum_{g \in G} g \in KG$. Prove that $< v >$ is the only trivial submodule of KG, where $< v >$ means the one dimensional subspace spanned by v.

(c) From (b), if KG were semi-simple, then ϵ would split the inclusion $< \sum_{g \in G} g > \subset KG$. Show that this gives a contradiction.

Therefore, we conclude (along with Maschke's theorem) that KG is a semi-simple ring $\iff$ char K does not divide $|G|$.

Defs/Thms 1. The group ring of G (over F is the free vector space over F with basis elements the elements of G and multiplication of basis elements same as multiplication in G ,extended by linearity.

1b. A typical element is a sum $\sum_{g \in G} \alpha_g g, \alpha_g \in F$, all but **finitely many** $\alpha_g = 0$.

2. (Maschke's Theorem) Let G be a finite group and F field whose characteristic does not divide $|G|$ (including char(F) = 0). If V is any FG- submodule and $U \leq V$ a submodule, then $\exists\, W \leq V$ submodule such that $U \oplus W = V$.

(i.e. every submodule of V is a direct summand).

3. There is an equivalence of categories Rep(G) $\cong$ FG- Mod.

3a. To a representation $\rho : G \to GL(V)$, we take the FG module to the set V with FG acting by:

$$g.v = \rho(g)(v) \text{ for } g \in G, v \in V$$

3b. To an FG - module V , we see V is a vector space by restriction of scalars along $F \leq FG$,defined by

$$\rho(g)(v) = g.v \text{ for } g \in G, v \in V.$$

4. Semisimple (or semisimple with minimum condition) satisfies Wedderburn's Theorem:

Let R be a nonzero ring with 1 (not necessarily commutative). Then FAE:

(i) every R-module is projective

(ii) every R-module is injective

(iii) every R-module is completely reducible.

(iv) the ring R considered as a left R-module is a direct sum

$$R = L_1 \oplus L_2 \oplus ... \oplus L_n$$

where each L_i is a simple module (i.e. simple left module) with $L_i = Re_i$ for some $e_i \in R$ with

(1) $e_i e_j = 0$ if $i \neq j$

(2) $e_i^2 = e_i$ for all i

(3) $\sum_{i=1}^n e_i = 1$

Proof First we prove that ϵ is a ring homomorphism.

(a-i) For $\alpha_g, \beta_g \in K, g \in G$, we first consider $\epsilon(\sum_{g \in G} \alpha_g g + \sum_{g \in G} \beta_g g)$. Then, we have:

$$\begin{aligned}
\epsilon(\sum_{g \in G} \alpha_g g + \sum_{g \in G} \beta_g g) &= \epsilon(\sum_{g \in G} (\alpha_g + \beta_g) g) \\
&= \sum_{g \in G} (\alpha_g + \beta_g) \\
&= \sum_{g \in G} \alpha_g + \sum_{g \in G} \beta_g \\
&= \epsilon(\sum_{g \in G} \alpha_g g) + \epsilon(\sum_{g \in G} \beta_g g)
\end{aligned}$$

(a-ii) Now consider $\epsilon(\sum_{g\in G}\alpha_g g \cdot \sum_{g\in G}\beta_g g)$.

The multiplication in group ring is defined as follows: $(ag_i)(bg_j) = (ab)g_k$ (D and F chapter 7.2). Then, we have the following:

$$\begin{aligned}\epsilon(\sum_{g\in G}\alpha_g g \cdot \sum_{g\in G}\beta_g g) &= \epsilon(\sum_{g_i g_j = g_k}\alpha_{g_i}\beta_{g_j} g)\\ &= \sum_{g\in G}\alpha_g\beta_g\\ &= \epsilon(\sum_{g\in G}\alpha_g g)\cdot\epsilon(\sum_{g\in G}\beta_g g)\end{aligned}$$

Hence, ϵ is a ring homomorphism.

(a-iii) Now, we show that ϵ is KG-module homomorphism. Let $r = \sum_{g\in G} r_g g, x = \sum_{g\in G} x_g g$. Then,

$$\begin{aligned}\epsilon(rx) &= \epsilon([\sum_{g\in G} r_g g][\sum_{g\in G} x_g g])\\ &= \epsilon(\sum_{g_i g_j = g_k} r_g x_g g)\\ &= \sum_{g_i g_j = g_k} r_g x_g\\ &= \sum_{g\in G} r_g \sum_{g\in G} x_g\\ &= \sum_{g\in G} r_g g \epsilon(\sum_{g\in G} x_g g)\\ &= r\epsilon(x)\end{aligned}$$

Hence, ϵ is a morphism of KG- modules.

(a-iv) Finally, we conclude that I is a 2-sided ideal of KG.

(By the First Isomorphism Theorems for Rings), If $\epsilon : KG \to K$ is a homomorphism of rings, then the kernel of ϵ is an ideal of KG.

Hence, $I = \ker(\epsilon)$ is a 2-sided ideal of KG.

(b-i) Suppose that $< v > = < \sum_{g\in G} g \leq KG$ is not trivial.

Know Since we are given the short exact sequence:

$$0 \to I \xrightarrow{i} KG \xrightarrow{\epsilon} K \to 0,$$

we know that (i) i is injective, (ii) ϵ is surjective, and (ii) im $(i) = \ker(\epsilon) = I$.

By one of the propositions corresponding to a split sequence, there exists a submodule $J \leq KG$ such that $KG = i(I) + J \Rightarrow KG \cong I \oplus J$.

(b-ii) Now, we show that $< v >$ is the only trivial submodule of KG.

Suppose there is another trivial submodule of KG, U where $u = \sum_{g \in G} \alpha_g g \in U$.

(From class), we can also think of KG as an K -algebra. So, consider $\alpha_g \in Z(KG)$. Then, consider the following:

(i) For a fixed $g' \in G$, since U is trivial, we have that:

$$g' \sum_{g \in G} \alpha_g g = \sum_{g \in G} \alpha_g g.$$

(ii) We also have:

$$g' \sum_{g \in G} \alpha_g g = \sum_{g \in G} g' \alpha_g g = \alpha_g (g' g)$$

(iii) Putting (i), (ii) together and reordering, we get:

$$\sum_{g \in G} \alpha_g (g' g) = \sum_{g \in G} \alpha_g g = \sum_{g \in G} \alpha_{g_2} g' g,$$

where g_2 is the new ordering.

Subtracting the first and third expressions we get the following:

(iv)

$$\sum_{g \in G} [\alpha_g (g' g) - \alpha_{g_2} (g' g)] = [\alpha_g - \alpha_{g_2}](g' g)$$

Since, both expressions are equal to $\sum_{g \in G} \alpha_g g$, in particular, we get: $[\alpha_g - \alpha_{g_2}](g' g) = 0 \iff \alpha_g = \alpha_{g_2}$.

(v) Let $\beta_g = \alpha_g - \alpha_{g_2}$. Then, we have

$$u = \sum_{g \in G} \beta_g g \in < v >$$

Since u is in the span of v , $< v > \leq KG$ is the only trivial submodule of KG.

(Source: Had a lot of help and hints from Zach on this one)

(c) By way of contradiction, suppose KG were semi-simple and ϵ split. Then, by part (b), the only trivial submodule is $v = \sum_{g \in G} g$.

Suppose K is a field of characteristic $p > 0$ and $p \Big| |G|$.

Then, we can write v as follows: $v = \sum_{g \in G} g = |G| = 0$, where the assertion follows since $p \Big| |G|$.

Similarly, for a fixed $k \in K, kv = 0 \Rightarrow kv \in \ker(\epsilon)$.

In particular, by part (b) $KG \cong J \oplus I$, where $J =< v >$. Since $kv \in \ker(\epsilon), J \leq I$.

This is a contradiction since we have the following:

$$KG \cong I \oplus J \Rightarrow KG/I \cong K \quad \text{since } J \leq I.$$

Hence, $p \Big| |G|$ if and only if KG is not semi-simple.
