8079 Semester 2, 2007

The University of Sydney

Faculties of Arts, Economics, Education,
Engineering and Science

MATH3966: Modules and Group Representations (Advanced)

Lecturer: Anthony Henderson

Time allowed: 2 hours plus 10 minutes reading time

This booklet contains **7** pages.

This paper comprises 6 questions worth a total of 70 marks.

All questions should be attempted. All working should be shown unless the question specifies otherwise. If you can't solve one part of a question, you can still assume the result in doing later parts.

No notes, books, or calculators are allowed.

SOLUTIONS

1. Throughout this question, R denotes a principal ideal domain.

(i) If $\{x_1, \cdots, x_s\}$ is a subset of an R-module M, what does it mean to say that M is *generated* by $\{x_1, \cdots, x_s\}$? (Give the definition.)

(ii) Suppose that M is an R-module and N is an R-submodule of M such that both N and M/N are finitely-generated R-modules. Prove that M is a finitely-generated R-module.

(iii) Either prove the following statement, or show it is false by giving a counter-example: if every finitely-generated R-module has a basis, then R is a field. (You may use any results from lectures that you find useful.)

(iv) Suppose that M is a nonzero R-module. What does it mean to say that M is *indecomposable*? (Give the definition.)

(v) Prove that R itself, regarded as an R-module, is indecomposable.

(vi) Give an example of a PID R and a non-unit element $r \in R$ such that the R-module R/Rr is decomposable.

[15 marks]

Solution:

(i) It means that every element of M can be written as an R-linear combination $r_1x_1 + \cdots + r_sx_s$ for some $r_1, \cdots, r_s \in R$.

(ii) Suppose that $x_1, \cdots, x_s$ generate N and $y_1 + N, \cdots, y_t + N$ generate M/N. For any $m \in M$, we can write $m+N$ as an R-linear combination $r_1(y_1+N)+\cdots+r_t(y_t + N)$ for some $r_1, \cdots, r_t \in R$. This means that

$$m - r_1y_1 - \cdots - r_ty_t \in N,$$

which implies that we can write $m - r_1y_1 - \cdots - r_ty_t$ as an R-linear combination $r'_1x_1 + \cdots + r'_sx_s$ for some $r'_1, \cdots, r'_s \in R$. So

$$m = r_1y_1 + \cdots + r_ty_t + r'_1x_1 + \cdots + r'_sx_s,$$

and we have shown that $\{x_1, \cdots, x_s, y_1, \cdots, y_t\}$ generates M.

(iii) Here is a proof. Suppose that every finitely-generated R-module is free (i.e. has a basis). Let r be any nonzero element of R, and consider the cyclic R-module R/Rr. Since R/Rr is free, it is torsion-free. But $r(1 + Rr) = 0 + Rr$, so we must have that $1 + Rr = 0 + Rr$, i.e. $1 \in Rr$. That is, r has an inverse. So R is a field.

(iv) It means that there are no nonzero R-submodules N and N' of M such that $M = N \oplus N'$.

(v) Suppose for a contradiction that $R = N \oplus N'$ for some nonzero R-submodules (i.e. ideals) N and N'. Let n be a nonzero element of N, and n' a nonzero element of N'. Then $nn' \in N \cap N' = \{0\}$, so $nn' = 0$, contradicting the assumption that R is an integral domain.

(vi) An example is $R = \mathbb{Z}$, $r = 6$: $\mathbb{Z}_6 = \{0, 2, 4\} \oplus \{0, 3\}$.

SOLUTIONS turn to page 3

2. In this question, you may use any of the general results proved in lectures.

(i) Show that the following integer matrix has invariant factors $2, 6, 0$:

$$A = \begin{pmatrix} 0 & 2 & 6 \\ 6 & 4 & 6 \\ 6 & 2 & 0 \end{pmatrix}.$$

(ii) Let M be the submodule of $\mathbb{Z}^3$ generated by the columns of the matrix A in the previous part. Is M a free $\mathbb{Z}$-module? Explain your answer.

(iii) Give the primary decomposition of the $\mathbb{Z}$-module $\mathbb{Z}^3/M$, where M is as in the previous part. That is, state an isomorphism between $\mathbb{Z}^3/M$ and a direct sum of indecomposable $\mathbb{Z}$-modules.

(iv) List all the $\mathbb{Z}$-modules with 36 elements, giving one representative of each isomorphism class. (No explanation is necessary.)

[10 marks]

Solution:

(i) Let the invariant factors be a_1, a_2, a_3. The gcd of the entries is clearly 2, so $a_1 = 2$. The 2×2 minors are -12, -12, -36, -12, -12, -36, -12, -12, and -36, whose gcd is 12, so $a_1 a_2 = 12$, proving that $a_2 = 6$. Finally, the determinant of the matrix is 0, so $a_1 a_2 a_3 = 0$, proving that $a_3 = 0$.

(ii) Yes, any submodule of a free finitely-generated $\mathbb{Z}$-module is free. In fact, the first two columns clearly form a basis for M.

(iii) Since the invariant factors of M in $\mathbb{Z}^3$ are 2 and 6, $\mathbb{Z}^3/M \cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}$. Now $\mathbb{Z}_6$ has primary decomposition $\mathbb{Z}_2 \oplus \mathbb{Z}_3$, so the primary decomposition of $\mathbb{Z}^3/M$ is $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}$.

(iv) Using the classification of finite $\mathbb{Z}$-modules (abelian groups) given in lectures, there are four isomorphism classes. Representatives are $\mathbb{Z}_4 \oplus \mathbb{Z}_9$, $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

turn to page 4

3. (*i*) Find the Jordan canonical form of the rational matrix

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 16 & -7 & -8 \\ -8 & 4 & 5 \end{pmatrix}.$$

(*ii*) Either prove the following statement, or show it is false by giving a counter-example: if $B \in \mathrm{Mat}_3(\mathbb{Q})$ has the same minimal polynomial as the matrix A in the previous part, then B is conjugate to A.

(*iii*) For any $\lambda \in \mathbb{C}$, let $J_n(\lambda)$ denote the Jordan block matrix

$$\begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{pmatrix} \in \mathrm{Mat}_n(\mathbb{C}).$$

Prove that if $\lambda \neq 0$, $J_n(\lambda)^2$ is conjugate to $J_n(\lambda^2)$. (*Hint – one of several possible methods*: first show that $J_n(\lambda)^2$ has characteristic polynomial $(x - \lambda^2)^n$, and then it suffices to prove that this is also its minimal polynomial.)

(*iv*) Hence prove that for every invertible complex matrix $A \in GL_n(\mathbb{C})$ there is an invertible matrix $B \in GL_n(\mathbb{C})$ such that $B^2 = A$.

[10 marks]

Solution:

(*i*) We calculate

$$\chi_A(x) = (x-1)\det\left(\begin{smallmatrix} x+7 & 8 \\ -4 & x-5 \end{smallmatrix}\right) = (x-1)(x^2+2x-3) = (x-1)^2(x+3).$$

To find the Jordan canonical form, we need to know whether the 1-eigenspace of A is one-dimensional or two-dimensional. By direct calculation, $\ker(A-1)$ has basis $\{(1,2,0),(1,0,2)\}$, so it is two-dimensional. Thus A is diagonalizable, and its Jordan canonical form is $\mathrm{diag}(1,1,-3)$. Its minimal polynomial is $(x-1)(x+3)$.

(*ii*) This is false: $\mathrm{diag}(1,-3,-3)$ also has minimal polynomial $(x-1)(x+3)$, and is not conjugate to A.

(*iii*) It is obvious that $J_n(\lambda)^2$ is upper-triangular with diagonal entries all equal to λ^2, so its characteristic polynomial is $(x-\lambda^2)^n$. Therefore its minimal polynomial is $(x-\lambda^2)^m$ for some $1 \leq m \leq n$. Since $((J_n(\lambda))^2 - \lambda^2)^m = 0$, the minimal polynomial of $J_n(\lambda)$, namely $(x-\lambda)^n$, must divide $(x^2-\lambda^2)^m = (x-\lambda)^m(x+\lambda)^m$. Since $\lambda \neq -\lambda$, this forces $m = n$. So $J_n(\lambda)^2$ is conjugate to $J_n(\lambda^2)$.

(*iv*) If $B^2 = A$ then $(XBX^{-1})^2 = XA^2X^{-1}$ for any $X \in GL_n(\mathbb{C})$, so it suffices to prove the result when A runs over a set of representatives for the conjugacy classes in $GL_n(\mathbb{C})$, for example the invertible matrices in Jordan canonical form. Since every complex number has a square root, the previous part shows that each Jordan block matrix with a nonzero eigenvalue has a square root. We can then arrange those square roots in the same block-diagonal form as the Jordan canonical form.

turn to page 5

4. In each part of this question, G is a finite group and V is a finite-dimensional $\mathbb{C}G$-module.

(i) Let W be a vector subspace of V. State the extra condition that W must satisfy in order to be a $\mathbb{C}G$-submodule of V.

(ii) Assuming that V is nonzero, say what it means for V to be a *simple* $\mathbb{C}G$-module (give the definition).

(iii) Either prove the following statement, or show it is false by giving a counter-example: if W is a $\mathbb{C}G$-submodule of V and $\sigma : V \to V$ is a $\mathbb{C}G$-module endomorphism, then $\sigma(W) \subseteq W$.

(iv) What does Schur's Lemma say about $\mathbb{C}G$-module endomorphisms of V in the case that V is simple? (State the result without proof.)

(v) Assume that G is abelian. Using the result of the previous part, prove that every simple $\mathbb{C}G$-module is 1-dimensional.

(vi) Using any results from lectures or tutorials, prove the converse of the previous part: if every simple $\mathbb{C}G$-module is 1-dimensional, then G is abelian.

[15 marks]

Solution:

(i) We must have that $gW \subseteq W$ (or equivalently, $gW = W$) for all $g \in G$.

(ii) V is simple if and only if it has no $\mathbb{C}G$-submodules other than $\{0\}$ and V.

(iii) A counter-example is $G = \{1\}$ (the trivial group). The statement asserts in this case that every linear transformation σ of a (finite-dimensional) complex vector space V preserves every subspace, which is obviously absurd.

(iv) It says that any $\mathbb{C}G$-module endomorphism of a simple finite-dimensional $\mathbb{C}G$-module is a scalar multiplication.

(v) Let V be a simple $\mathbb{C}G$-module with representation $T : G \to GL(V)$. Since G is abelian, each $T(g)$ is a $\mathbb{C}G$-module endomorphism of V, hence a scalar multiplication. Thus every subspace of V is a $\mathbb{C}G$-submodule. So V has no subspaces except $\{0\}$ and V, and therefore must be 1-dimensional.

(vi) Suppose that every simple $\mathbb{C}G$-module is 1-dimensional. Since the sum of the squares of the dimensions of the simple $\mathbb{C}G$-modules equals $|G|$, there must be $|G|$ simple $\mathbb{C}G$-modules (up to isomorphism). Therefore there are $|G|$ conjugacy classes in G, i.e. every element is in its own conjugacy class, i.e. G is abelian.

5. In this question n is an integer ≥ 2, F is a finite field, and $G = GL_n(F)$ is the group of $n \times n$ invertible matrices over the field F.

(i) Show that the rule

$$T(g)(A) = gAg^{-1}, \text{ for all } g \in G,\ A \in \mathrm{Mat}_n(F),$$

defines a representation T of G on $\mathrm{Mat}_n(F)$.

 turn to page 6

(*ii*) As a consequence of part (*i*), $\mathrm{Mat}_n(F)$ is an FG-module. Show that

$$\{A \in \mathrm{Mat}_n(F) \mid \mathrm{tr}(A) = 0\}$$

is an FG-submodule of $\mathrm{Mat}_n(F)$.
(*iii*) Assuming that the characteristic of the field F does not divide n, show that $\mathrm{Mat}_n(F)$ has an FG-submodule which is complementary to the one in part (*ii*). (*Warning*: Maschke's Theorem does not apply, because the characteristic of F divides $|G|$.)

[10 marks]

Solution:

(*i*) It is clear that $T(g)(A)$ is linear in A, so the rule defines a map $T : G \to \mathrm{End}(\mathrm{Mat}_n(F))$. Moreover, $T(1) = 1$ because $1A1^{-1} = A$, and $T(gh) = T(g)T(h)$ because $(gh)A(gh)^{-1} = g(hAh^{-1})g^{-1}$. This shows that the image of T lies in $GL(\mathrm{Mat}_n(F))$ and that T is a representation.
(*ii*) Since $\mathrm{tr} : \mathrm{Mat}_n(F) \to F$ is a nonzero linear function, its kernel is a subspace of $\mathrm{Mat}_n(F)$ of codimension 1. To show that it is an FG-submodule, we must show that $\mathrm{tr}(A) = 0 \Rightarrow \mathrm{tr}(gAg^{-1}) = 0$ for any $g \in G$; this is clear, because trace is unchanged under conjugation.
(*iii*) Since $g1_ng^{-1} = 1_n$ for all $g \in G$, $F1_n$ is a one-dimensional FG-submodule of $\mathrm{Mat}_n(F)$. The assumption on characteristic implies that $\mathrm{tr}(1_n) = n \neq 0$, so $F1_n$ is not contained in the submodule found in the previous part; considering their dimensions, the two submodules must be complementary.

6. Let G be the group with presentation

$$\langle x, y \mid x^6 = 1,\, y^4 = 1,\, x^3 = y^2,\, yxy^{-1} = x^{-1}\rangle.$$

You may assume that it has 12 elements, divided into 6 conjugacy classes as follows:

$$\{1\},\ \{x, x^5\},\ \{x^2, x^4\},\ \{x^3\},\ \{y, x^2y, x^4y\},\ \{xy, x^3y, x^5y\}.$$

Hence there are 6 isomorphism classes of simple $\mathbb{C}G$-modules.

(*i*) Find the complete character table of G, explaining all your reasoning. (*Hint:* it may be useful, though it is not necessary, to prove that there is a surjective homomorphism $G \to S_3$.)
(*ii*) Using any valid method, determine which of the simple $\mathbb{C}G$-modules are defined over $\mathbb{R}$.
(*iii*) Hence or otherwise, find the number of equivalence classes of representations of G on $\mathbb{R}^2$.

[10 marks]

Solution:

turn to page 7

(i) We first find the one-dimensional characters, i.e. group homomorphisms $\psi : G \to \mathbb{C}^\times$. The relation $\psi(y)\psi(x)\psi(y)^{-1} = \psi(x)^{-1}$ implies that $\psi(x) = 1$ or -1. In the first case, $\psi(x)^3 = \psi(y)^2$ shows that $\psi(y) = \pm 1$; in the second case, it shows that $\psi(y) = \pm i$. Each of these four possibilities gives a one-dimensional character: these are in fact the powers $1, \psi^2, \psi, \psi^3$ where $\psi(y) = i$. The remaining two simple $\mathbb{C}G$-modules must both be two-dimensional, because the sum of the squares of the dimensions is $|G| = 12$. Let χ be one of their characters. If $\psi\chi = \chi$, then χ must vanish except on the identity (value 2) and the class of x^2 (value a, say); but then the orthogonality $\langle \chi, 1 \rangle = 0$ would force $a = -1$, which would make $\langle \chi, \chi \rangle = \frac{1}{2}$, a contradiction. Hence $\psi\chi$ is the character of the other two-dimensional simple module, and $\psi^2\chi = \chi$. The values of χ must be $2, a, b, c, 0, 0$ for some a, b, c, meaning that the values of $\psi\chi$ are $2, -a, -b, c, 0, 0$. Orthogonality of the first and fourth columns forces $c = -1$. The orthogonality relation $\langle \chi, 1 \rangle = 0$ implies $2 + a + 2b - 2 = 0$, so $a = -2b$. Since x is conjugate to its inverse, the values of all characters on it are real, so $b \in \mathbb{R}$. Then orthogonality of the second and third columns says that $4 - 4b^2 = 0$, so $b = \pm 1$. The choice of ± 1 is a matter of renaming χ and $\psi\chi$, so we can assume that $b = 1$. The character table is:

	1	x^3	x	x^2	y	xy
	1	1	2	2	3	3
1	1	1	1	1	1	1
ψ	1	-1	-1	1	i	$-i$
ψ^2	1	1	1	1	-1	-1
ψ^3	1	-1	-1	1	$-i$	i
χ	2	-2	1	-1	0	0
$\psi\chi$	2	2	-1	-1	0	0

(ii) A one-dimensional simple $\mathbb{C}G$-module is defined over $\mathbb{R}$ if and only if its character is real-valued, which is true for 1 and ψ^2 but not for ψ or ψ^3. For the two-dimensional simple $\mathbb{C}G$-modules, we compute Frobenius-Schur indicators:

$$FS(\chi) = \frac{1}{12}(1 \times 2 + 1 \times 2 + 2 \times (-1) + 2 \times (-1) + 3 \times (-2) + 3 \times (-2)) = -1,$$
$$FS(\psi\chi) = \frac{1}{12}(1 \times 2 + 1 \times 2 + 2 \times (-1) + 2 \times (-1) + 3 \times 2 + 3 \times 2) = 1.$$

So the simple module with character $\psi\chi$ is defined over $\mathbb{R}$, and that with character χ is not.

(iii) The previous part shows that the characters of the simple $\mathbb{R}G$-modules are 1 and ψ^2 (one-dimensional), $\psi + \psi^3$ and $\psi\chi$ (two-dimensional), and 2χ (four-dimensional). Hence there are five isomorphism classes of two-dimensional $\mathbb{R}G$-modules: $\mathbb{R} \oplus \mathbb{R}$, $\mathbb{R} \oplus \mathbb{R}_{\psi^2}$, $\mathbb{R}_{\psi^2} \oplus \mathbb{R}_{\psi^2}$, and the two simple ones. This is equivalent to saying that there are five equivalence classes of representations of G on $\mathbb{R}^2$.