MAT 314: FINAL EXAM SOLUTIONS

MAY 21, 2019

1. Let M be the module over the ring $R = \mathbb{C}[x]$, which is 4-dimensional as a vector space over $\mathbb{C}$, and with action of x given by the matrix

$$A = \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Write M in the form

$$M = \bigoplus_i \mathbb{C}[x]/(p_i^{n_i}),$$

where $p_i \in \mathbb{C}[x]$ are irreducible.

Solution.

Note that the matrix $\begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}$ is diagonalizable (it has two distinct eigenvalues), and the diagonalized matrix is $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$.

Thus, Jordan canonical form of A is

$$A = \begin{bmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

and the corresponding module is

$$M = \mathbb{C}[x]/(x-2)^2 \oplus \mathbb{C}[x]/(x-2) \oplus \mathbb{C}[x]/(x-1)$$

Common mistakes.

Several students wrote that $\mathbb{C}[x]/(x-2)^2 \oplus \mathbb{C}[x]/(x-2) = \mathbb{C}[x]/(x-2)^3$. This is incorrect, for the same reason as $\mathbb{Z}/p^3$ is not the same as $\mathbb{Z}/p^2 \oplus \mathbb{Z}/p$.

---

2. Let G be the abelian group generated by three generators x_1, x_2, x_3 with relations

$$\begin{aligned} 3x_1 + x_2 + 2x_3 &= 0 \\ x_1 + x_2 + x_3 &= 0 \\ 2x_1 + 3x_2 + 6x_3 &= 0 \end{aligned}$$

Describe G as a product of cyclic groups.

Solution.

This system of generators and realtions can be described by the matrix

$$\begin{bmatrix} 3 & 1 & 1 \\ 1 & 1 & 1 \\ 2 & 3 & 6 \end{bmatrix}$$

By elementary row and column operations (over $\mathbb{Z}$!), this matrix can be reduced to

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 7 \end{bmatrix}$$

Thus, the corresponding abelian group is

$$G = \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z} = \mathbb{Z}_7$$

---

3. Let D_n be the dihedral group, i.e. the group of all symmetries of a regular n-gon. It is known that this group is generated by two elements x (rotation by $2\pi/n$) and y (reflection), with the following relations:

$$x^n = y^2 = 1, \qquad yxy^{-1} = x^{-1}.$$

In parts (a)–(c) below, V is a finite-dimensional complex representation of G; we denote by $\rho(x)$, $\rho(y)$ the action of $x, y \in D_n$ in V.

(a) Show that in any representation V, the operator $\rho(x)$ is diagonalizable. What are the possible eigenvalues of this operator? [Hint: subgroup generated by x is the cyclic group...]

(b) Let $v \in V$ be an eigenvector for $\rho(x)$ with eigenvalue λ. Show that then $v' = \rho(y)v$ is also an eigenvector for $\rho(x)$, with eigenvalue λ^{-1}, and that the subspace V' generated by v, v' is a subrepresentation.

(c) Classify all irreducible representations of D_n.

Solution.

(a) The subgroup generated by x is the cyclic group $\mathbb{Z}_n$; thus, if we just consider V with action of x, forgetting about y, we get a representation of the cyclic group $\mathbb{Z}_n$. As we had proved before, any such representation can be written as direct sum of one-dimensional subrepresentations, which is equivalent to saying that there is a basis in which $\rho(x)$ is diagonal. Since $\rho(x)^n v = v$ for any v, this implies that for any eigenvalue λ, $\lambda^n = 1$, so every eigenvalue must be an n-th root of unity.

(b) Since $xy = yx^{-1}$ in D_n, we have

$$\rho(x)v' = \rho(x)\rho(y)v = \rho(y)\rho(x^{-1})v = \rho(y)\lambda^{-1}v = \lambda^{-1}v'$$

Therefore, we have

$$\begin{aligned} \rho(x)v = \lambda v, \quad \rho(x)v' = \lambda^{-1}v' \\ \rho(y)v = v', \quad \rho(y)v' = v \end{aligned}$$

which implies that for any $g \in D_n$, $\rho(g)V' \subset V'$.

(c) From parts (a), (b), any representation has a subrepresentation generated by two vectors v, v'. Thus, any irreducible representation is either one-dimensional (if v, v' are linearly dependent, which implies that we must have $\lambda = \lambda^{-1}$) or two-dimensional (if v, v' are linearly independent). Full list is below:

- One-dimensional irreducible representations: $V = \mathbb{C}$, $\rho(y) = \pm 1$, $\rho(x) = 1$ (if n is odd) or $\rho(x) = \pm 1$ (if n is even). For even n, signs can be chosen independently, which gives in this case 4 irreducible one-dimensional representations
- Two dimensional irreducible representations: for any λ such that $\lambda^n = 1$, $\lambda \neq \pm 1$, we have a two-dimenisonal irreducible representation V_λ with basis v_1, v_2 and action of x, y given by

$$\rho(x)v_1 = \lambda v_1, \quad \rho(x)v_2 = \lambda^{-1}v_2$$
$$\rho(y)v_1 = v_2, \quad \rho(y)v_2 = v_1$$

Note that $V_\lambda \simeq V_{\lambda^{-1}}$.

Comments.
Few people got part (c), but this was expected. What was unexpected is that very few people got part (a). Some students wrote that $\rho(x)$ is diagonalizable because it is invertible, which is completely wrong.

---

4. Let $\alpha = \sqrt{10 + 5\sqrt{2}}$.

(a) Find the degree of α over $\mathbb{Q}$ and the minimal polynomial.
(b) Determine the Galois group of that minimal polynomial over $\mathbb{Q}$.
(c) Can α be written in the form $\sqrt{a} + \sqrt{b}$, with $a, b \in \mathbb{Q}$? [Hint: this would imply $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{a}, \sqrt{b})$.]

Solution.

(a) One easily sees that $\alpha^2 = 10 + 5\sqrt{2}$, so $(\alpha^2 - 10)^2 = (5\sqrt{2})^2 = 50$. This shows that α is a root of

$$p(x) = x^4 - 20x^2 + 50.$$

This shows that $[\mathbb{Q}[\alpha) : \mathbb{Q}] \leq 4$. On the other hand, $\alpha^2 = 10 + 5\sqrt{2}$ implies that $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\alpha)$, and it is easy to show that α can not be written in the form $a + b\sqrt{2}$, so this is a proper subfield. Therefore, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ and $p(x)$ is irreducible.

(b) The roots of $p(x)$ are

$$\alpha_1 = \alpha = \sqrt{10 + 5\sqrt{2}}$$
$$\alpha_2 = \sqrt{10 - 5\sqrt{2}}$$
$$\alpha_3 = -\alpha$$
$$\alpha_4 = -\alpha_2$$

Observe that

$$\alpha_1\alpha_2 = \sqrt{50} = 5\sqrt{2}$$

and since $\sqrt{2} \in \mathbb{Q}(\alpha)$, this implies that $\alpha_2 = \alpha_1/(5\sqrt{2}) \in \mathbb{Q}(\alpha)$. Therefore, all four roots are in $\mathbb{Q}(\alpha)$, so the splitting field is $\mathbb{Q}(\alpha)$ and the Galois group $G = Gal(\mathbb{Q}(\alpha)/\mathbb{Q})$ has order 4, so it can be either $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_4$.

Let $s \in G$ be the automorphism such that $s(\alpha_1) = \alpha_2$ (it exists because they are roots of the same irreducible polynomial). Note that then $s(\alpha_1^2) = \alpha_2^2$, which implies $s(\sqrt{2}) = -\sqrt{2}$. Therefore,

$$s(\alpha_2) = s\Big(\frac{\alpha_1}{5\sqrt{2}}\Big) = \frac{\alpha_2}{-5\sqrt{2}} = -\alpha_1$$

which easily implies that s permutes the four roots cyclically:

$$\alpha_1 \to \alpha_2 \to -\alpha_1 \to -\alpha_2 \to \alpha_1$$

and thus has order 4. Therefore, $G = \mathbb{Z}_4$

(c) If $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{a}, \sqrt{b})$, it means that $[\mathbb{Q}(\sqrt{a}, \sqrt{b}) : \mathbb{Q}] = 4$, so $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{a}, \sqrt{b})$. But we had shown that in such situations, the Galois group $Gal(\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}) = \mathbb{Z}_2 \times \mathbb{Z}_2$, which contradicts part (b). Therefore, it is impossible.

Comments.
Common mistakes were:

- saying that the splitting filed is $\mathbb{Q}(\alpha)$ without a proof
- saying "let s be an element of the Galois group such that $s(\alpha_1) = \alpha_2$, $s(\alpha_2) = \alpha_1$". You need to expalin why such an element exists — not every permutation of roots can be obtained from the Galois group. In fact, as the argument above shows, such an element in this case doesn't exist.

Note that part (c) can be done without use of the Galois group; this was accepted as a correct solution.

---

5. Let L be the splitting field of the polynomial $x^6 + 1$ over $\mathbb{Q}$.

(a) What is the degree $[L : \mathbb{Q}]$?

(b) Describe the Galois group $G = Gal(L/\mathbb{Q})$, both as an abstract group (e.g. by generators and relations) and as a subgroup in S_6.

(c) Now let K be the splitting field of the polynomial $x^2 + 1$ over $\mathbb{Q}$. Prove that then $\mathbb{Q} \subset K \subset L$, and describe the corresponding subgroup $H \subset G$ as prescribed by the main theorem of Galois theory.

Solution.

(a) Let $\zeta = e^{2\pi i/12}$ be the primitive 12th root of unity. Then $\zeta^6 = e^{\pi i} = -1$, so ζ is one of the roots of $x^6 + 1$ and thus is in L. Moreover, it is easy to see that the other roots are $\zeta^3 = i, \zeta^5, \zeta^7, \zeta^9 = -i, \zeta^{11} = \zeta^{-1}$ (all odd powers of ζ). Therefore, $L = \mathbb{Q}(\zeta)$, so $[L : \mathbb{Q}] = \varphi(12) = 4$.

(b) From known results about cyclotomic polynomials and cyclotomic extensions, $Gal(L/\mathbb{Q}) = \mathbb{Z}_{12}^*$. If we consider $s_1, s_2 \in G$ defined by

$$s_1(\zeta) = \zeta^{-1}$$
$$s_2(\zeta) = \zeta^5$$

then one easily sees that $s_1^2 = s_2^2 = 1$, $s_1 s_2 = s_2 s_1$, so $G = \mathbb{Z}_2 \times \mathbb{Z}_2$.

Numbering roots of $x^6 + 1$ as follows:

$$\begin{aligned}
\alpha_1 &= \zeta \\
\alpha_2 &= \zeta^5 \\
\alpha_3 &= \zeta^{-1} \\
\alpha_4 &= \zeta^7 = \zeta^{-5} \\
\alpha_5 &= \zeta^3 = i \\
\alpha_5 &= \zeta^9 = -i
\end{aligned}$$

we see that s_1, s_2 are permutations

$$\begin{aligned}
s_1 &= (13)(24)(56) \in S_6 \\
s_2 &= (12)(34) \in S_6
\end{aligned}$$

(note that $s_2(\alpha_5) = (\zeta^3)^5 = \zeta^3 = \alpha_5$).

(c) The corresponding subgroup must be a group of order 2, so $H \simeq \mathbb{Z}_2$ is the subgroup generated by s_2.