Kayla Orlinsky

Algebra Exam Fall 2016

Problem 1. If $R := \mathbb{C}[x, y]/(y^2 - x^3 - 1)$, then describe all the maximal ideals in R.

Solution. By the correspondence theorem, there is a 1-to-1 correspondence between maximal ideals of R and maximal ideals of $\mathbb{C}[x, y]$ containing $(y^2 - x^3 - 1)$.

By Nullstellensatz, maximal ideals of $\mathbb{C}[x, y]$ are of the form $(x - a, y - b)$ for some $a, b \in \mathbb{C}$.

Now, again by Nullstellensatz, $a, b \in \mathbb{C}$ must be such that $(a, b) \in V(y^2 - x^3 - 1)$. Namely, the maximal ideals of R correspond exactly to $(a, \pm\sqrt{a^3 + 1})$ where $a \in \mathbb{C}$. ✌

Problem 2. Suppose F is a field, and $\mathfrak{b}_n(F)$ is the F-algebra of upper-triangular matrices, i.e., the subalgebra of $M_n(F)$ consisting of matrices X such that $X_{ij} = 0$ when $i > j$. Describe the Jacobson radical of $\mathfrak{b}_n(F)$, the simple modules, and the maximal semi-simple quotient.

Solution. Let $A = \mathfrak{b}_n(F)$.

$\boxed{J(A)}$ Note that A is finite dimensional over F and so $J(A)$ is nilpotent.

Now, if $X \in J(A)$ then X is noninvertible, however, because $J(A)$ is quasi-regular, $I - X$ has a left inverse in A.

Namely, X has a 0 eigenvalue while $I - X$ does not. Since the eigenvalues of upper triangular matrices are exactly the values down the main diagonal, we get that 1 is not an eigenvalue of X, else $I - X$ has a 0 eigenvalue.

However, $aX \in J(A)$ for $a \in F$, and so if X has any non-zero eigenvalue λ then $\lambda^{-1}X \in J(A)$ has 1 as an eigenvalue. This contradicts that $I - \lambda^{-1}X$ is invertible since this matrix will have a 0 down the main diagonal.

Namely, X cannot have any non-zero eigenvalues.

Therefore, every matrix in $J(A)$ has zeros down the main diagonal.

Now, if Y is a matrix that has zeros down the main diagonal, then Y has only 0s as an Eigenvalue so $Y^n = 0$ by Cayley Hamilton. Thus, Y is nilpotent.

Since all nilpotent ideals are contained in $J(A)$, we have that $Y \in J(A)$.

Namely, $J(A)$ is exactly the set of strictly upper triangular matrices, or upper triangular matrices with zeros down the main diagonal.

$\boxed{\text{Simple modules}}$ A simple module of A is a simple left A-module, namely a quotient of A by a maximal left ideal.

Since maximal left ideals are exactly

$$I_i = \{X \in A \,|\, (X)_{ij} = 0, j = 1, ..., n\}$$

namely, the matrices in A with the i^{th} column zeros, we have that $A/I_i \cong F^i$ where $i = 1, ..., n$.

$\boxed{\text{Maximal Semi-simple Quotient}}$ I believe that we are being asked to find is an ideal $I \subset A$ such that the quotient A/I is semi-simple and A/I is the largest of these quotients.

This will clearly be $A/J(A)$.

Since A is artinian A/I is artinian for all ideals I (quotients of artinian rings are artinian).

Now, A/I is semi-simple if and only if A/I artinian and $J(A/I) = 0$ by Artin Wedderburn.

Since there is a 1-to-1 correspondence between maximal ideals of A containing I and maximal ideals of A/I, we see that $J(A/I) = 0$ implies that the intersection of every maximal ideal of A/I is contained in I. Therefore, the intersection of all maximal ideals containing I

is contained in I and so $J(A) \subset I$. Finally, A/I is isomorphic to a subset of $A/J(A)$ and so $A/J(A)$ is maximal.

✌

Problem 3. Let $\mathbb{F}_5$ be the finite field with 5 elements, and consider the group $G = PGL_2(\mathbb{F}_5)$ (i.e., the quotient of the group of invertible 2×2 matrices over $\mathbb{F}_5$ by the subgroup of scalar multiple of the identity.

(a) What is the order of G?

(b) Describe $N_G(P)$ where P is a Sylow 5-subgroup of G.

(c) If $H \subset G$ is a subgroup, can H have order $15, 20, 30$?

Solution.

(a)

$$|GL_2(\mathbb{F}_5)| = (5^2-1)(5^2-5) = (25-1)\cdot(25-5) = 24\cdot 20 = 8\cdot 3\cdot 5\cdot 4 = 2^5\cdot 3\cdot 5.$$

Now, scalar multiples of the identity is of course a subgroup of size $5-1=4$ so

$$|PGL_2(\mathbb{F}_5)| = 2^5\cdot 3\cdot 5/2^2 = 2^3\cdot 3\cdot 5 = 120 = 5!$$

(b) Let P be a Sylow 5-subgroup of G.

By Sylow, the number of Sylow 5-subgroups of G, n_5 satisfies that $n_5 | 2^3\cdot 3$ and $n_5 \equiv 1 \mod 5$. Therefore, $n_5 = 1, 6$.

Now, in G, scalar multiples of the identity are the same. Namely,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} xa & xb \\ xc & xd \end{bmatrix} \in G \qquad x \in \mathbb{F}_5.$$

Thus,

$$\begin{aligned} \begin{bmatrix} 2 & 4 \\ 0 & 2 \end{bmatrix}^2 &= \begin{bmatrix} 4 & 1 \\ 0 & 4 \end{bmatrix} \\ \begin{bmatrix} 2 & 4 \\ 0 & 2 \end{bmatrix}^5 &= \begin{bmatrix} 4 & 1 \\ 0 & 4 \end{bmatrix}\begin{bmatrix} 4 & 1 \\ 0 & 4 \end{bmatrix}\begin{bmatrix} 2 & 4 \\ 0 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 2 & 4 \\ 0 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \\ &= I \end{aligned}$$

Therefore,

$$P = \left\langle \begin{bmatrix} 2 & 4 \\ 0 & 2 \end{bmatrix} \right\rangle$$

is a Sylow 5-subgroup.

Now,

$$\begin{bmatrix} 0 & 2 \\ 3 & 0 \end{bmatrix} \begin{bmatrix} 0 & 2 \\ 3 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

so $\begin{bmatrix} 0 & 2 \\ 3 & 0 \end{bmatrix}$ is its own inverse. However,

$$\begin{aligned} \begin{bmatrix} 0 & 2 \\ 3 & 0 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 0 & 2 \\ 3 & 0 \end{bmatrix} &= \begin{bmatrix} 0 & 4 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 0 & 2 \\ 3 & 0 \end{bmatrix} \\ &= \begin{bmatrix} 2 & 0 \\ 1 & 2 \end{bmatrix} \end{aligned}$$

which is not an element of P. Therefore, $N_G(P) \neq G$ so $n_5 = 6$ and

$$|N_G(P)| = 120/6 = 20.$$

Since the normalizers will be isomorphic by the conjugation isomoprhism (because Sylow p-subgroups are all conjugates), it suffices to examine $N_G(P)$ where P is the Sylow 5-subgroup given above.

Note

$$\begin{aligned} \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix}^{-1} &= \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} \\ &= \begin{bmatrix} 2 & 4 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} \\ &= \begin{bmatrix} 2 & 1 0 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 3 0 & 1 \end{bmatrix} \in P \end{aligned}$$

so $\begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} \in N_G(P)$.

Now,

$$\begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 4 \\ 0 & 3 \end{bmatrix} \neq \begin{bmatrix} 2 & 4 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 0 & 3 \end{bmatrix}$$

so $N_G(P)$ is non-abelian.

Now, it is quickly verified that

$$\begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 4 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ 0 & 4 \end{bmatrix} \in P$$

so $\begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} \in N_G(P)$ and has order 4. Therefore, $N_G(P)$ is a non-abelian group of order 20 which Sylow 2-subgroups isomorphic to $\mathbb{Z}_4$.

Therefore, $N_G(P)$ is a semi-direct product.

Let $\varphi : \mathbb{Z}_4 \to \text{Aut}(\mathbb{Z}_5)$. Then if $\mathbb{Z}_4 \cong \langle a \rangle$ and $\mathbb{Z}_5 \cong \langle b \rangle$, $\varphi_i(a) = \sigma_i$ $i = 1, 2, 3$ where $\sigma_1(b) = b^2$, $\sigma_2(b) = b^3$ and $\sigma_3(b) = b^4$.

Clearly $\sigma_1^3 = \sigma_2$ so $\varphi_1(a^3) = \varphi_2(a)$. Since $a \mapsto a^3$ is an isomorphism of $\mathbb{Z}_4$, the following diagram commutes and so φ_1 and φ_2 generate isomorphic semi-direct products.

$$\begin{tikzcd}
\langle a \rangle \arrow[r, "\varphi_2"] \arrow[d, "a\mapsto a^3"'] & \text{Aut}(\mathbb{Z}_5) \\
\langle a \rangle \arrow[ur, "\varphi_1"'] &
\end{tikzcd}$$

Now, this gives two possible multiplications for $N_G(P)$, either through φ_1 or φ_3. Namely,

$$N_G(P) \cong \langle a, b \,|\, a^4 = b^5 = 1, aba^{-1} = b^2 \rangle$$

$$N_G(P) \cong \langle a, b \,|\, a^4 = b^5 = 1, aba^{-1} = b^4 \rangle$$

Thus, we need only check if an element a of order 4 and a generator b of P satisfy $ab = b^2a$ or $ab = b^{-1}a$.

Since

$$ab = \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} \begin{bmatrix} 2 & 4 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 4 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 3 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 1 \\ 0 & 4 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix} = b^2a$$

we have at last that

$$N_G(P) \cong \langle a, b \,|\, a^4 = b^5 = 1, aba^{-1} = b^2 \rangle$$

> ***Note that $PGL_2(\mathbb{F}_5) \cong S_5$, so perhaps showing such an isomoprhism would allow us to reach the conclusion of (b) faster.

(c) $\boxed{20}$ Let $H \subset G$ be a subgroup. First, $|N_G(P)| = 20$ so $|H| = 20$ is fine.

$\boxed{15}$ Now, assume that H has order 15. Then H necessarily contains a Sylow 5-subgroup P. However, $|H| = 15$ so $n_5|3$ and $n_5 \equiv 1 \mod 5$ implies that $n_5 = 1$ where n_5 here is the number of Sylow 5-subgroups of H. Namely, P is normal in H.

However, if $g \in G$ normalizes P, then $g \in N_G(P)$ by definition, thus $H \subset N_G(P)$. However, $|N_G(P)| = 20$ and so it does not have any elements of order 3, namely H cannot be a subset of $N_G(P)$.

Thus, H does not exist.

$\boxed{30}$ Now, let H have order 30. By the same argument as before, H cannot have only one normal Sylow 5 subgroup, and so it must contain all 6 Sylow 5 subgroups since by Sylow, $n_5|6 = |H|/5$ and $n_5 \equiv 1 \mod 5$.

Now, we note that in H, $n_3 \equiv 1 \mod 3$ and $n_3|10$. Thus, $n_3 = 1, 10$. Since H contains all the Sylow 5 subgroups of G, it cannot contain 10 Sylow 3-subgroups. Since every

Sylow 5-subgroup has order 5 and every Sylow 3-subgroup has order 3, and since by the Sylow theorems, Sylow p-subgroups are all conjugates of each other, for each p, this would force H to have $4 \cdot 6$ non-trivial elements of order 5 and $2 \cdot 10$ non-trivial elements of order 3. Since this is $4 \cdot 6 + 2 \cdot 10 = 24 + 20 = 44$ distinct non-trivial elements and H has order 30, we reach a contradiction.

Thus, H has one normal Sylow 3-subgroup Q. However, then for any Sylow 5-subgroup P of H, PQ will be a subgroup of H of order 15.

Namely, then G will have a subgroup of order 15. Since this is not possible we are done.

✌

Problem 4. Let A be an $n \times n$ matrix over $\mathbb{Z}$. Let V be the $\mathbb{Z}$-module of column vectors of size n over $\mathbb{Z}$.

(a) Prove that the size of V/AV is equal to the absolute value of $\det(A)$ if $\det(A) \neq 0$.

(b) Prove that V/AV is infinite if $\det(A) = 0$.

(hint: use the theory of finitely generated modules $\mathbb{Z}$-modules)

Solution.

(a) We use that A has a smith normal form (since $\mathbb{Z}$ is a PID). Namely, there exists invertible matrices P, Q so $A = PDQ$ and D is diagonal. Since P, Q are inverible over $\mathbb{Z}$, $\det(P) = \pm 1$ and $\det(Q) = \pm 1$.

Namely, $\det(A) = \pm \det(D)$.

Now, $V = \mathbb{Z}e_1 \oplus \cdot \oplus \mathbb{Z}e_n$ where e_i is the standard basis vector with 1 in the i^{th} position.

Now, because P, Q are invertible, $QV = V$ and $PV = V$ so

$$AV = PDQV = PDV = DV.$$

If

$$D = \begin{bmatrix} d_1 & 0 & \cdots & 0 & 0 \\ 0 & d_2 & \cdots & 0 & 0 \\ & \vdots & \cdots & \vdots & \\ 0 & 0 & \cdots & d_{n-1} & 0 \\ 0 & 0 & \cdots & 0 & d_n \end{bmatrix}$$

then

$$V/DV = \mathbb{Z}/(d_1)e_1 \oplus \cdots \oplus \mathbb{Z}/(d_n)e_n \cong \mathbb{Z}_{d_1}e_1 \oplus \cdots \oplus \mathbb{Z}_{d_n}e_n.$$

Namely, $|V/DV| = |d_1 \cdot d_2 \cdot \cdots \cdot d_n| = |\det(D)| = |\det(A)|$.

(b) Note that $\mathbb{Z}$ is a PID. Thus, by the structure theorem of finitely generated modules over a PID,

$$V = \mathbb{Z}^n \oplus T(V)$$

where $T(V)$ is the torsion part of V.

Note that the rank of the free part of V has size n since there are n linearly independent vectors of length n over $\mathbb{Z}$, namely the standard basis vectors.

If $\det(A) = 0$, then the columns of A cannot span $\mathbb{Z}^n$.

Therefore,

$$AV = \mathbb{Z}^m \oplus T(AV)$$

where $m < n$ and $T(AV)$ is the torsion part of AV. Namely, V/AV will have at least one copy of $\mathbb{Z}$ in its decomposition. Namely, it will be infinite.

Again, this follows since rank(V/AV) =rank$(V)-$rank$(AV) > 0$.

✌

Problem 5. Let V be a finite dimensional right module over a division ring D. Let W be a D-submodule of V.

(a) Let $I(W) = \{f \in \mathrm{End}_D(V) \,|\, f(W) = 0\}$. Prove that $I(W)$ is a left ideal of $\mathrm{End}(V)$.

(b) Prove that any left ideal of $\mathrm{End}_D(V)$ is $I(W)$ for some submodule W.

Solution.

(a) $I(W)$ is nonempty, it contains the 0 map. Let $f, g \in I(W)$ then by linearity, $(f - g)(W) = f(W) - g(W) = 0 + 0 = 0$ so $f - g \in I(W)$. Thus, $I(W)$ is closed as an additive abelian group.

Now, let $h \in \mathrm{End}(V)$. Then "multiplication" is actually composition in $\mathrm{End}(V)$ so if $f \in I(W)$ then
$$(hf)(W) = (h \circ f)(W) = h(f(W)) = h(0) = 0$$
because h is an endomorphism and so preserves the origin.

Thus, $hf \in I(W)$ so $I(W)$ is a left ideal.

(b) Let J be any left ideal of $\mathrm{End}_D(V)$. Note that V is finite dimensional so there exists $v_i \in V$ so
$$V = v_1 D + \cdots v_n D.$$

Let
$$W = \bigcap_{f \in J} \ker(f).$$

Note that $0 \in W$ so W is nonempty. Then, $W \subset V$. If $x, y \in W$ and $f \in J$ then
$$f(x - y) = f(x) - f(y) = 0 - 0 = 0$$
so $x - y \in W$.

If $a \in D$ then
$$f(ax) = af(x) = 0$$
so $ax \in W$.

Now, clearly $J \subset I(W)$ since every $f \in J$ satisfies that $f(W) = 0$.

Let $g \in I(W)$.

Let $f_i \in J$ such that $f_i(v_i) \neq 0$. Note that if $f(v_i) = 0$ for all $f \in J$, then $v_i \in W$ so $g(v_i) = 0$.

Now, let $h_i \in \mathrm{End}(V)$ such that $h_i(f(v_i)) = g(v_i)$ and $h_i(f(v_j)) = 0$ for all $j \neq i$. If $g(v_i) = 0$ then take $h_i \equiv 0$.

Let $x \in V$, then

$$x = \sum_{i=1}^{n} a_i v_i \qquad a_i \in D.$$

Thus,

$$\begin{aligned}
\sum_{j=1}^{n} (h_j \circ f_j)(x) &= \sum_{j=1}^{n} (h_j \circ f_j) \left(\sum_{i=1}^{n} a_i v_i \right) \\
&= \sum_{j=1}^{n} \sum_{i=1}^{n} (h_j \circ f_j)(a_i v_i) \\
&= \sum_{j=1}^{n} \sum_{i=1}^{n} a_i h_j(f_j(v_i)) \\
&= \sum_{j=1}^{n} a_j h_j(f_j(v_j)) \\
&= \sum_{j=1}^{n} a_j g(v_j) \\
&= g \left(\sum_{j=1}^{n} a_j v_j \right) \\
&= g(x)
\end{aligned}$$

Therefore,

$$g = \sum_{j=1}^{n} (h_j \circ f_j) \in J$$

so $I(W) \subset J$.

✌

Problem 6. Let p and q be distinct primes. Let F be the subfield of $\mathbb{C}$ generated by the pq-roots of unity. Let a, b be squarefree integers all greater than 1. Let $c, d \in \mathbb{C}$ with $c^p = a$ and $d^q = b$. Let $K = F(c, d)$.

(a) Show that $K/\mathbb{Q}$ is a Galois extension.

(b) Describe the Galois group K/F

(c) Show that any intermediate field $F \subset L \subset K$ satisfies $L = F(S)$ where S is some subset of $\{c, d\}$.

Solution.

(a) Let ξ be a primitive pq^{th}-root of unity in F. Then

$$\xi^{pq} = (\xi^p)^q = 1$$

so F contains a primitive p^{th}-root of unity as well. Similarly, it contains a primitive q^{th} root of unity.

We claim that K is the splitting field of $f(x) = (x^p - a)(x^q - b)$. Clearly c, d satisfy these polynomials. Now, if α is a root of $f(x)$, then $\alpha^p = a$, or $\alpha^q = b$. Thus, $\alpha = c(\xi^q)^t$ or $d(\xi^p)^s$ for some t or some s so $\alpha \in K$.

Thus, $f(x)$ splits completely over K so K is the splitting field of a separable polynomial over $\mathbb{Q}$ so $K/\mathbb{Q}$ is Galois.

(b) Since $[K : \mathbb{Q}] \leq pq$, and

$$[K : \mathbb{Q}] = [K : F(c)][F(c) : \mathbb{Q}] = [K : F(c)]p$$

and

$$[K : \mathbb{Q}] = [K : F(d)][F(d) : \mathbb{Q}] = [K : F(d)]q$$

we have that $[K : \mathbb{Q}] = pq$.

Thus, $G = \text{Gal}(K/\mathbb{Q})$ has order pq. WLOG, take $p < q$.

Now, let $\sigma, \tau \in G$ be defined by $\sigma(c) = c\xi^q$ and $\sigma(d) = d$, and $\tau(c) = c$ and $\tau(d) = d\xi^p$. Then σ clearly has order p and τ has order q.

Furthermore, σ and τ commute so any permutation of the roots of $f(x)$ will be given by some power of σ and τ.

Specifically, the map $c \mapsto c(\xi^q)^i$ and $d \mapsto d(\xi^p)^j$ is given by $\sigma^i\tau^j$.

Therefore, G is abelian and so it is isomoprhic to $\mathbb{Z}_{pq}$.

(c) By the Galois correspondence theorem, each intermediate field $F \subset L \subset K$ corresponds to a subgroup H of G where $|H| = [K : L]$. Since if $H \neq G, \{e\}$, we have that $|H| = p, q$, we have that $[K : L] = p, q$.

Since G is abelian, there are exactly two nontrivial proper subgroups H of order p and q. Therefore, there are two field extensions of F contained strictly in K. Since $F(c)$ and $F(d)$ are two such extensions, these must be the only two.

✌