ALGEBRA QUALIFYING EXAM FALL 2010

Do all six problems. Each problem is worth 4 points and partial credit may be awarded.

1. Use Sylow's Theorems to show that any group of order $(99^2 - 4)^3$ is solvable.

2. For any finite group G and positive integer m, let $n_G(m)$ be the number of elements g of G that satisfy $g^m = e_G$. If A and B are finite abelian groups so that $n_A(m) = n_B(m)$ for all m, show that as groups $A \cong B$.

3. If $g(x) = x^5 + 2 \in \boldsymbol{Q}[x]$, for $\boldsymbol{Q}$ the field of rational numbers, compute the Galois group of a splitting field L over $\boldsymbol{Q}$ of $g(x)$. How many subfields of L containing $\boldsymbol{Q}$ are Galois over $\boldsymbol{Q}$?

4. Let P be a minimal prime ideal in the commutative ring R with 1; that is, if Q is a prime ideal in R and if $Q \subseteq P$, then $Q = P$. Show that each $x \in P$ is a zero divisor in R.

5. Set $R = \boldsymbol{C}[x_1, \ldots, x_n]$ with $n \geq 3$ and $\boldsymbol{C}$ the field of complex numbers. For any subset $S \subseteq R$, let $\mathcal{V}(S) = \{\alpha \in \boldsymbol{C}^n \mid g(\alpha) = 0 \text{ for all } g \in S\}$. Consider the ideal I of R defined by $I = (x_1 \cdots x_{n-1} - x_n,\ x_1 \cdots x_{n-2}x_n - x_{n-2}, \ldots, x_2 \cdots x_n - x_1)$, so the generators of I are obtained by subtracting each x_j from the product of the others. Show that there are fixed positive integers s and t so that for each $0 \leq i \leq n$, $(x_i^s - x_i)^t \in I$. (Hint: Consider the product of the generators of I.)

6. Let R be a right artinian algebra over an algebraically closed field F. Show that R is algebraic over F of bounded degree. That is, show there is a fixed positive integer m so that for any $r \in R$ there is a nonzero $g_r(x) \in F[x]$ with $g_r(r) = 0$ and with $\deg g \leq m$.

Algebra Fall 2010

(1) Prove using Sylow's theorems that any group of order $(99^2-4)^3$ is solvable.

---

solution

$$|G| = 101^3 \cdot 97^3.$$

By the primality test, 97 & 101 are primes.

$n_{101} = 1, \cancel{97}, 97^2, 97^3$
$\equiv 1 \pmod{101}$

$n_{97} = 1, \cancel{101}, \cancel{101^2}, \cancel{101^3}$
$\equiv 1 \pmod{97}$

$101 \equiv 4$
$101^2 \equiv 16$
$101^3 \equiv 64$

Hence the 97-Sylow subgroup N is normal. N is solvable since it is a p-group. $|G/N| = 101^3$ hence G/N is solvable since it is a p-group. Therefore, G is solvable. $\square$

(2) For a positive integer m let $n_G(m) = \# \{ g \in G : g^m = e_G \}$. If A and B are finite abelian s.t. $n_A(m) = n_B(m)$ for all m, show $A \cong B$.

---

solution

write $A \cong \bigoplus_{\substack{i \in I_A \\ j_i \in J_A^i}} \mathbb{Z}/p_i^{n_{ij_i}}\mathbb{Z}$ and $B \cong \bigoplus_{\substack{i \in I_B \\ j_i \in J_B^i}} \mathbb{Z}/q_i^{m_{ij_i}}\mathbb{Z}$.

Assume for each i, $n_{i1} \leq n_{i2} \leq \cdots \leq n_{ij_i^A}$ and similarly for m. Then $n_A(n_{1j_1^A} \cdots n_{i_A j_i^A}) = |A|$ equals $n_B(n_{1j_1^A} \cdots n_{ij_i^A}) \leq |B|$. Conversely, $|A| \geq |B|$. So $|A| = |B|$.

It is better to write

$A \cong \mathbb{Z}/d_1 \oplus \cdots \oplus \mathbb{Z}/d_n \qquad d_1 | d_2 | \cdots | d_n$

$B \cong \mathbb{Z}/d_1' \oplus \cdots \oplus \mathbb{Z}/d_{n'}' \qquad d_1' | d_2' | \cdots | d_n'$

If $n_A(m) = |A|$, then $d_n \leq m$. We have $n_B(d_{n'}') = |B| = |A|$ equals $n_A(d_{n'}')$. So $d_n \leq d_{n'}'$. Conversely, $d_{n'}' \leq d_n$.

So $d_n = d'_{n'}$. Let $A \cong \tilde{A} \oplus \mathbb{Z}/d_n$.

We claim $n_A(m) = n_{\tilde{A}}(m)\, n_{\mathbb{Z}/d_n}(m)$.

The general elt of A is $(\tilde{a}, n)$. If $m\tilde{a} = 0$ and $mn = 0$, then $m(\tilde{a}, n) = 0$; and vice versa. The former gives "$\geq$" while the latter gives "$\leq$".

And similarly for $B \cong \tilde{B} \oplus \mathbb{Z}/d_n$.

$$\begin{array}{ccc} \text{So} \quad n_A(m) & = & n_B(m) \\ \| & & \| \\ n_{\tilde{A}}(m)\, n_{\mathbb{Z}/d_n}(m) & & n_{\tilde{B}}(m)\, n_{\mathbb{Z}/d_n}(m) \end{array}$$

So $n_{\tilde{A}}(m) = n_{\tilde{B}}(m)$ for all m.

By induction on n, $B \cong \tilde{\tilde{B}} \oplus A$.

But $|B| = |A|$ implies $\tilde{\tilde{B}} = 0$. $\square$

(3) Let $g(X) = X^5 + 2$, viewed in $\mathbb{Q}[X]$.
Compute the Galois group of $g(X)$, i.e. the Galois group of the splitting field L of $g(X)$ over $\mathbb{Q}$. How many subfields of L containing $\mathbb{Q}$ are Galois over $\mathbb{Q}$?

<u>solution</u>

$L = \mathbb{Q}(\sqrt[5]{2}, \delta)$ where δ is a primitive 5^{th} root of unity.

$[\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 5$ since $X^5 - 2$ is irreducible by Eisenstein.

$[\mathbb{Q}(\delta) : \mathbb{Q}] = 4$ w/ minimal poly $\underset{\Phi_5(x)}{\overset{\shortparallel}{X^4 + X^3 + X^2 + X + 1}}$.

so $5 \mid [L, \mathbb{Q}]$ and $4 \mid [L : \mathbb{Q}] \Rightarrow 20 \mid [L:\mathbb{Q}]$

and $[L : \mathbb{Q}] \leq 5 \cdot 4 = 20$.

so $[L : \mathbb{Q}] = 20$.

so $|G| = 20$.

Since $\Phi_5(x)$ irred / $\mathbb{Q}(\sqrt[5]{2})$

(as $[L:\mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{2}):\mathbb{Q}][L:\mathbb{Q}(\sqrt[5]{2})]$)

we get an elt of $\mathrm{Aut}(L : \mathbb{Q}(\sqrt[5]{2})) \subset G$

by sending $\begin{cases} \delta \mapsto \delta^n \\ \sqrt[5]{2} \mapsto \sqrt[5]{2} \end{cases}$ $n = 1, 2, 3, 4$

i.e. $\mathrm{Aut}\, \mathbb{Z}/5 \cong \underset{\substack{\parallel\!\wr \\ H}}{\mathbb{Z}/4} \subset G,$

w/ generator $\varphi : \begin{cases} \delta \mapsto \delta^2 \\ \sqrt[5]{2} \mapsto \sqrt[5]{2} \end{cases}$.

Since $x^5 - 2$ irred / $\mathbb{Q}(\delta)$

we get an elt of $\mathrm{Aut}(L : \mathbb{Q}(\delta)) \subset G$

by sending $\begin{cases} \delta \mapsto \delta \\ \sqrt[5]{2} \mapsto \delta^n \sqrt[5]{2} \end{cases}$ $n = 0, 1, \ldots, 4$

i.e. $\overset{K}{\underset{}{\mathbb{Z}/5}} \subset G$ w/ generator $\psi : \begin{cases} \delta \mapsto \delta \\ \sqrt[5]{2} \mapsto \delta(\sqrt[5]{2}) \end{cases}$

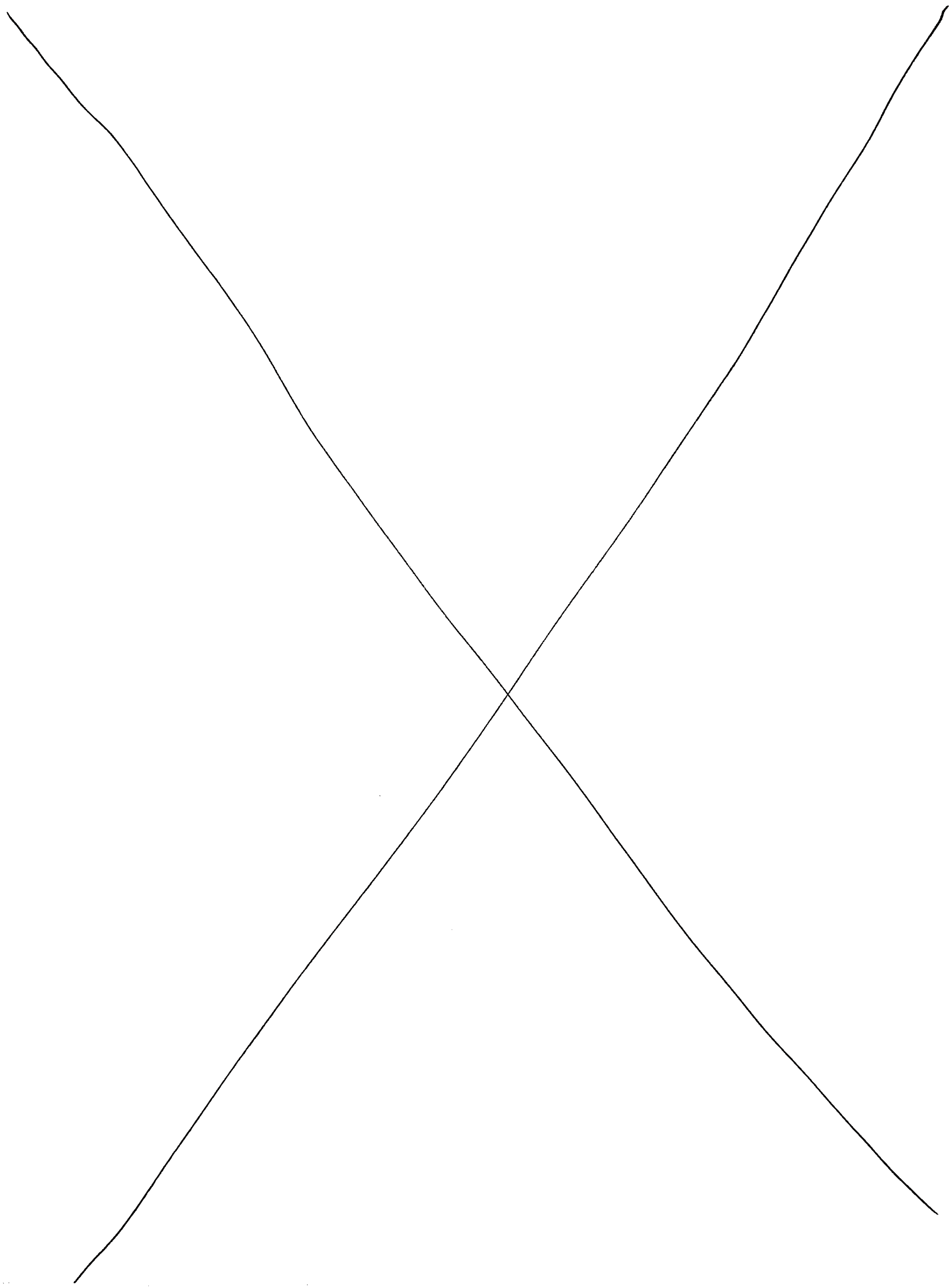
Note: $H \cap K = \{e\}$ so $G \cong H \rtimes K$ — Note: K is normal.

And $\varphi^{-1} : \begin{cases} \delta \mapsto \delta^3 \\ \sqrt[5]{2} \mapsto \sqrt[5]{2} \end{cases}$

so $\varphi\psi\varphi^{-1} : \begin{cases} \delta \mapsto \delta^3 \mapsto \delta^3 \mapsto \delta \\ \sqrt[5]{2} \mapsto \sqrt[5]{2} \mapsto \delta(\sqrt[5]{2}) \mapsto \delta^2(\sqrt[5]{2}). \end{cases}$ so $\varphi\psi\varphi^{-1} = \psi^2$.

so $G \cong \langle x, y : x^4 = y^5 = 1,\ xyx^{-1} = y^2 \rangle$ a nonabelian group of order 20.

~~The subgroups of G are $\{e\}, H, K, G$ all of which are normal. So there are 4 Galois extensions over $\mathbb{Q}$ in L.~~ $\blacksquare$



$$G \cong \langle X, y : X^4 = y^5 = 1,\ Xy = y^2X \rangle.$$

- nonabelian group of order 20.
- general elt y^iX^j. $\begin{pmatrix} i = 0,1,\dots,4 \\ j = 0,1,\dots,3 \end{pmatrix}$.

- subgroups of order 1 : $\{1\}$. normal.
- subgroups of order 5: $\{1, y, y^2, y^3, y^4\}$. normal.
- subgroups of order 4: $\{1, X, X^2, X^3\}$, $\{1, yX, y^3X^2, y^2X^3\}$, $\{1, y^2X, yX^2, y^4X^3\}$, $\{1, y^3X, y^4X^2, yX^3\}$, $\{1, y^4X, y^2X^2, y^3X^3\}$.
- subgroups of order 2: $\{1, X^2\}$, $\{1, y^3X^2\}$, $\{1, yX^2\}$, $\{1, y^2X^2\}$.
- subgroups of order 10: $\{1, y, y^2, y^3, y^4, X^2, yX^2, y^2X^2, y^3X^2, y^4X^2\}$ normal.
- subgroups of order 20: G normal

$\longrightarrow$ $K = \langle y \rangle$ fixes $\mathbb{Q}(\delta)$ so $K \subset Gal(L/\mathbb{Q}(\delta))$.
Since $[G : Gal(L/\mathbb{Q}(\delta))] = [\mathbb{Q}(\delta) : \mathbb{Q}] = 4$, we have $K = Gal(L/\mathbb{Q}(\delta))$. Since $\mathbb{Q}(\delta)/\mathbb{Q}$ is Galois, as all the roots of $\Phi_5(X)$ are in $\mathbb{Q}(\delta)$, we have K is normal.

$H = \langle X \rangle$ fixes $\mathbb{Q}(\sqrt[5]{2})$ so $H \subset Gal(L/\mathbb{Q}(\sqrt[5]{2}))$.
Since $[G : Gal(L/\mathbb{Q}(\sqrt[5]{2}))] = [\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 5$, we have $H = Gal(L/\mathbb{Q}(\sqrt[5]{2}))$. Since $\mathbb{Q}(\sqrt[5]{2})/\mathbb{Q}$ is not Galois, as the roots $\sqrt[5]{2}\,\delta^i$ $(i = 1,2,3)$ of $X^5 - 2$ are not in $\mathbb{Q}(\sqrt[5]{2})$, we have H is not normal.

By Sylow, there are five subgroups $\cong H \cong \mathbb{Z}/4$. The subgroups of order 2 are not normal because they can be conjugated into any copy of $\mathbb{Z}/4$ by Sylow, and each copy of $\mathbb{Z}/4$ has a different elt of order 2. The unique subgroup of order 10 is normal since its index is 2. We conclude there are precisely four subfields of L which are Galois over $\mathbb{Q}$.

$\square$

---

(4) Let P be a minimal prime ideal in a commutative ring R w/ 1, i.e. if $Q \subset P$ is prime, then $Q = P$. Show every $x \in P$ is a zero divisor in R.

~~<u>solution</u> Let $I = \{r \in R : r \in P$ and r is a 0-divisor$\}$.~~
~~We show I is a prime ideal, hence every elt of P is a 0-divisor. If $a, b \in I$, then $au = bv = 0$ for some $u, v \in R$, $u, v \neq 0$. So since R is comm, $(a+b)\overbrace{uv}^{\text{not necessarily nonzero}} = 0$, so $a+b \in I$. And for all $r \in R$, $(ra)u = 0$, so $ra \in I$. So I is an ideal. If $ab \in I$ then there is $w \in R$ s.t. $(ab)w = 0$. Since $ab \in P$, either $a \in P$ or $b \in P$. In the former, $a(bw) = 0$ so $a \in I$ and in the latter $b(aw) = 0$ so $b \in I$. So $I \subset P$ is prime.~~

solution

Since p is a minimal prime, the localization R_p has the unique prime $pR_p = \left\{ \frac{rp}{s} : \begin{array}{l} r \in R \\ p \in P \\ s \notin P \end{array} \right\}$.

Since the nilradical is the intersection of primes, every elt of pR_p is nilpotent. So $p^n = 0 \in R_p$.

Take the minimal such n. By definition, this means there is $t \notin P$ s.t. $tp^n = 0 \in R$.

Since n is minimal, $tp^{n-1} \neq 0$. Hence p is a zero divisor.

$\square$

---

5 Let $R = \mathbb{C}[X_1, \dots, X_n]$ where $n \geq 3$.

Let $V(I) \subset \mathbb{C}^n$ denote the vanishing set of an ideal $I \subset R$.
Let $J(A) \subset R$ denote the polynomials vanishing on a set $A \subset \mathbb{C}^n$.

Consider $I = (X_1 \cdots X_{n-1} - X_n, X_1 \cdots X_{n-2} X_n - X_{n-1}, \dots, X_2 \cdots X_n - X_1)$.

Show there are positive integers s and t s.t. for each $1 \leq i \leq n$, we have $(X_i^s - X_i)^t \in I$.

---

solution Proof in the specific case $n = 3$:

$V(I)$ is determined by solving $\begin{cases} X_1X_2 = X_3 \\ X_1X_3 = X_2 \\ X_2X_3 = X_1 \end{cases}$. The origin is a solution and $X_i \neq 0$ implies $X_j \neq 0$ for all $j \neq i$. We see $X_1^2 X_3 = X_3 \Rightarrow X_1^2 = 1$.

Similarly $X_2^2 = 1$ and $X_3^2 = 1$. More precisely,

$$\begin{cases} X_1 X_2 = X_3 \\ X_1 X_3 = X_2 \\ X_2 X_3 = X_1 \end{cases} \iff \begin{cases} X_1^2 = 1 \\ X_3^2 = 1 \\ X_2 X_3 = X_1 \end{cases}$$

and we have the additional overall constraint $X_i^2 = 1$.

we may solve the system fully choosing any square root of 1 for X_1 and X_3.

Now, to say $(X_i^s - X_i)^t \in I$ means $(X_i^s - X_i) \in \sqrt{I} = J(V(I))$, i.e. $X_i^s - X_i$ vanishes on the zero locus of I. Thus Taking $s = 3$ we have $(X_i^s - X_i)^{t_i} \in I$. Taking $t = \max_i t_i$ we have $(X_i^s - X_i)^t \in I$ for all i, as desired.

<u>we see now how to generalize:</u>

Assume $X_i \neq 0$ and

$$\begin{cases} X_1 \cdots X_{n-1} = X_n \\ X_1 \cdots X_{n-2} X_n = X_{n-1} \\ \quad \vdots \qquad\qquad \vdots \\ X_2 \cdots X_n = X_1 \end{cases}.$$

~~Plugging in eq for~~ $\cancel{X_{n-1}}$ ~~into that for~~ $\cancel{X_n}$ ~~gives~~ $\cancel{X_1^2 \cdots X_{n-2}^2 = 1}$.

~~Plugging in eq for~~ $\cancel{X_k}$ ~~into that for~~ $\cancel{X_{k+1}}$ ~~gives~~ $\cancel{X_1^2 \cdots X_{k-1}^2 X_{k+2}^2 \cdots X_n^2 = 1}$.

~~We show by induction on~~ $\cancel{n}$ ~~that this implies~~ $\cancel{X_i}$

It is clear this implies for any $i_1, i_2, \ldots, i_{n-2}$ that $X_{i_1}^2 X_{i_2}^2 \cdots X_{i_{n-2}}^2 = 1$.

~~We start from here by induction on that~~ $\cancel{X_i}$

$$\therefore \quad \frac{X_1^2 \cancel{X_3^2} \cdots \cancel{X_{n-1}^2}}{X_2^2 \cancel{X_3^2} \cdots \cancel{X_{n-1}^2}} = 1, \quad \frac{\cancel{X_1^2} X_2^2 \cancel{X_4^2} \cdots \cancel{X_{n-1}^2}}{\cancel{X_1^2} X_3^2 \cancel{X_4^2} \cdots \cancel{X_{n-1}^2}} = 1, \quad \ldots,$$

$$\frac{\cancel{X_1^2} \cdots \cancel{X_{n-3}^2}\, X_n^2}{\cancel{X_1^2} \cdots \cancel{X_{n-3}^2}\, X_{n-1}^2} = 1.$$

Hence $\quad X_1^2 = X_2^2 = \cdots = X_n^2$.

Hence, plugging into $X_3^2 \cdots X_n^2 = 1$, we have $X_i^{2(n-2)} = 1$ for all i.

So $s = 2(n-2).+1$

The rest of the proof is identical to the case $n = 3$. $\square$

---

(6) A right Artinian algebra over alg closed field F.

Assume in addition that A/F is algebraic.

Show that A is algebraic over F of bounded degree, i.e. there is a positive integer m s.t. for any $r \in A$ there is a nonzero $g_r(X) \in F[X]$ s.t. $g_r(r) = 0$ and $\deg g \le m$.

---

solution Let J denote the Jacobson radical of A.

Special case: A is semisimple

We may assume $A = M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$.

Since A is an F-alg, there is a map $F \to Z(A)$ into the center of A.

Since
$$Z(A) = Z(M_{n_1}(D_1)) \times \cdots \times Z(M_{n_k}(D_k))$$
$$= Z(D_1) \times \cdots \times Z(D_k),$$
by projecting onto the i^{th} component we get a map $F \to Z(D_i)$, hence $D_i \subset A$ is an F-alg and is thus algebraic over F since A is.

We show $D_i = F$: If $\alpha \in D_i$, then there is a poly $f(X) \in F[X]$ s.t. $f(\alpha) = 0$.

But since D_i is a divison alg, $f(X)$ viewed in $D[X]$ has at most $d \equiv \dim f$ roots in D. Thus, since F is alg closed, all the roots of f in D lie in F. In particular, $\alpha \in F$. ✓

So $A = M_{n_1}(F) \times \cdots \times M_{n_k}(F)$. Let $(A_1, \ldots, A_k) \in A$. Let $f_i \in F[X]$ be the char poly of A_i. Then $f \equiv f_1 \cdots f_k \in F[X]$ is the desired poly. So A is algebraic of bounded degree $\leq n_1 \cdots n_k$. ✓

General case

Since A is right Artinian,

A/J is semisimple, and clearly satisfies the hypotheses of the special case.

So it suffices to show all elements of J satisfy polynomials of bounded degree.

Since A is right Artinian, J is nilpotent.

So in fact every $r \in J$ satisfies a poly X^N for N fixed.

$\square$.