ALGEBRA QUALIFYING EXAM FALL 2005

Work all the problems. Be as explicit as possible in your solutions and justify your statements with specific reference to the results that you use. Partial credit will be given for partial solutions.

1. Let G be a group with $|G| = p^n q^m$ for $p < q$ primes and assume that the order of $[p]_q$ in the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^*$ is larger than n. Show that there are subgroups $\langle e \rangle \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H_{n+m} = G$ with each $H_j \lhd H_{j+1}$ and H_{j+1}/H_j cyclic of prime order.

2. Let $F \subseteq L$ be finite fields with $[L : F] = 3$. If $\alpha \in F$ show that there is $\beta \in L$ satisfying $\beta^3 = \alpha$.

3. If $p(x) = x^8 + 6x^4 + 1 \in \mathbb{Q}[x]$ and if $\mathbb{Q} \subseteq M \subseteq C$ is a splitting field for $p(x)$ over $\mathbb{Q}$, argue that $\mathrm{Gal}(M/\mathbb{Q})$ is solvable.

4. Let R be a commutative ring with 1 and let $x_1, \ldots, x_n \in R$ so that $x_1 y_1 + \cdots + x_n y_n = 1$ for some $y_j \in R$. Let $A = \{(r_1, \ldots, r_n) \in R^n \mid x_1 r_1 + \cdots + x_n r_n = 0\}$. Show that $R^n \cong_R A \oplus R$, that A has n generators as an R module, and that when $R = F[x]$ for F a field then A_R is free of rank $n - 1$.

5. Let $R = C[x_1, \ldots, x_n]$ and let I be a nonzero proper ideal of R. If $A \in M_k(R)$ and $A(\alpha) = 0_{k \times k}$ for all $\alpha \in \mathrm{Var}(I)$, show that for some $s > 0$, $A^s \in M_k(I)$.

6. If R is a right Artinian algebra over C, show there is an integer $m \geq 1$ so that if $x \in R$ and $x^k = 0$ for some integer $k \geq 1$, then $x^m = 0$: that is, the indices of nilpotence of the nil elements of R are bounded.

Def'n: R comm rng w/ 1.

An R-algebra is a ring A with hom $f: R \to A$, $1_R \mapsto 1_A$ and $f(R) \subseteq Z(A) \subseteq A$

Algebra - Fall 2005:

① $|G| = p^n q^m$, $p<q$ primes, and $\text{ord}_q(p) > n$ in $\mathbb{Z}_q^*$.
Show that there are subgroups $\langle e\rangle \leq H_1 \leq H_2 \leq \cdots \leq H_{n+m} = G$ with each $H_j \trianglelefteq H_{j+1}$ & H_{j+1}/H_j cyclic of prime order.

By Sylow, $r_q \equiv 1 \pmod q$ & $r_q \mid p^n \Rightarrow r_q = p^k$ for some $k \leq n$, but $\text{ord}(p) > n$ in $\mathbb{Z}_q^*$, hence $p^k \not\equiv 1 \pmod q$ for all $k \leq n$, hence $r_q = 1$. Therefore the Sylow q-subgroup is normal in G, call it $Q \trianglelefteq G$.

Now, $Q \trianglelefteq G$ and $|Q| = q^m$; hence $|G/Q| = p^n$, hence Q & G/Q are finite p-groups, hence both are solvable; Q & G/Q solvable, hence G solvable, so such a series exists. Let $P = G/Q$.

- Q solvable $\Rightarrow \exists \langle e\rangle \trianglelefteq A_1 \trianglelefteq A_2 \trianglelefteq \cdots \trianglelefteq A_k = Q$ with A_{i+1}/A_i prime order.
$\Rightarrow A_{i+1}/A_i \cong \mathbb{Z}_q \Rightarrow |A_{i+1}| = q^{j+1}$, $|A_i| = q^j$

Hence $|A_i| = q^i$, so we have $k = m$, hence:

$$\langle e\rangle \trianglelefteq A_1 \trianglelefteq \cdots \trianglelefteq A_m = Q.$$

- P solvable $\Rightarrow \exists \langle e\rangle \trianglelefteq B_1 \trianglelefteq \cdots \trianglelefteq B_l = P$ with B_{i+1}/B_i prime order
$\Rightarrow B_{i+1}/B_i \cong \mathbb{Z}_p \Rightarrow |B_{i+1}| = p^{j+1}$, $|B_i| = p^j$

Hence $l = n$ and $|B_i| = q^j$, hence:

$$\langle e\rangle \trianglelefteq B_1 \trianglelefteq \cdots \trianglelefteq B_n = P$$

orders coprime ↓

$$\Rightarrow Q \trianglelefteq B_1 Q \trianglelefteq \cdots \trianglelefteq B_n Q = PQ \cong G$$

$$\Rightarrow \langle e\rangle \trianglelefteq A_1 \trianglelefteq \cdots \trianglelefteq A_m = Q \trianglelefteq B_1 Q \trianglelefteq \cdots \trianglelefteq B_n Q = PQ \cong G$$

Hence let $H_i = A_i$, $i = 1, \ldots, m$ and $H_j = B_j Q$ for $j = m+1, \ldots, m+n$.

Hence solvable series length $n+m$ exists.

(2) $F \subseteq L$ finite fields, $[L:F]=3$, $\alpha \in F$

Show that $\exists \beta \in L$ such that $\beta^3 = \alpha$:

Since F, L finite fields and $[L:F]=3$, we must have $F \cong \mathbb{F}_q$ & $L \cong \mathbb{F}_{q^3}$ where $q = p^n$. Since $\mathbb{F}_q^\times$ & $\mathbb{F}_{q^3}^\times$ are finite multiplicative subgroups of a field, they are cyclic, so let $\langle x \rangle = \mathbb{F}_{q^3}^\times$.

Now consider the map $\varphi : \mathbb{F}_{q^3}^\times \longrightarrow \mathbb{F}_{q^3}^\times$

$$g \longmapsto g^3$$

If $3 \nmid q^3-1 = |\mathbb{F}_{q^3}^\times|$, then x^3 is also a generator of $\mathbb{F}_{q^3}^\times$, hence φ is surjective, hence since $F^\times \subseteq \mathbb{F}_q^\times \subseteq \mathbb{F}_{q^3}^\times = L^\times$, all nonzero elements $\alpha \in F \subseteq L$ have some $\beta \in L$ s/t $\varphi(\beta) = \alpha \Rightarrow \underline{\beta^3 = \alpha}$.

If $3 \mid q^3-1$: then $3 \mid (q-1)(q^2+q+1)$; 3 prime so $3 \mid (q-1)$ or $3 \mid (q^2+q+1)$. Now, $\varphi(L^\times) = \varphi(\mathbb{F}_{q^3}^\times)$ is a cyclic group of order $\frac{q^3-1}{3}$. If $(q-1) \mid \frac{q^3-1}{3}$ then $\mathbb{F}_q^\times$ is a subgroup of $\operatorname{im}\varphi = \varphi(L^\times)$, hence $\alpha \in \mathbb{F}_q^\times$ has $\alpha = \varphi(\beta) = \beta^3$ for $\beta \in L^\times$.

Case 1: $3 \mid q^2+q+1$

then $\frac{q^3-1}{3} = (q-1)\left(\frac{q^2+q+1}{3}\right) \Rightarrow \underline{(q-1) \mid \frac{q^3-1}{3}}$ ✓

Case 2: $3 \mid q-1$

then $q \equiv 1 \pmod 3 \Rightarrow q^2 \equiv 1 \pmod 3$

$\Rightarrow q^2+1 \equiv 2 \pmod 3$

$\Rightarrow q^2+q+1 \equiv 3 \pmod 3 \Rightarrow q^2+q+1 \equiv 0 \pmod 3$

$\Rightarrow 3 \mid q^2+q+1$

$\Rightarrow$ case 1 $\Rightarrow \underline{(q-1) \mid \frac{q^2-1}{3}}$

✓

③ $p(x)=x^8+6x^4+1 \in \mathbb{Q}[x]$, $\mathbb{Q} \subseteq M \subseteq \mathbb{C}$ splitting field

Show that $Gal(M/\mathbb{Q})$ solvable

See that $p(x) = x^8+6x^4+1 = (x^4)^2+6(x^4)+1 \Rightarrow x^4 = \frac{-6 \pm \sqrt{36-4}}{2}$

$= \frac{-6 \pm \sqrt{32}}{2} = \frac{-6 \pm 4\sqrt{2}}{2}$

$= -3 \pm 2\sqrt{2}$

Let $\alpha = -3+2\sqrt{2}$ & $\overline{\alpha} = -3-2\sqrt{2}$

Then $i^j \sqrt[4]{\alpha}$ & $i^j \sqrt[4]{\overline{\alpha}}$ where $j = 1, -1, 4$ are the roots.

So then $\mathbb{Q}(i, \sqrt[4]{\alpha}, \sqrt[4]{\overline{\alpha}})$ is the splitting field. M

Then see that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(i, \sqrt[4]{\alpha}, \sqrt[4]{\overline{\alpha}})$

Now since $i^4 = 1$, $(\sqrt[4]{\alpha})^4 = \alpha$, $(\sqrt[4]{\overline{\alpha}})^4 = \overline{\alpha} \in \mathbb{Q}(\sqrt{2})$, we have

hence $\mathbb{Q}(i, \sqrt[4]{\alpha}, \sqrt[4]{\overline{\alpha}})/\mathbb{Q}(\sqrt{2})$ is radical; clearly $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is radical.

Therefore $\mathbb{Q}(i, \sqrt[4]{\alpha}, \sqrt[4]{\overline{\alpha}})/\mathbb{Q}$ radical, hence $Gal(M/\mathbb{Q})$ is solvable.

④ R comm ring w/ 1. Let $x_1, \dots, x_n \in R$ such that $x_1y_1 + \cdots + x_ny_n = 1$ for some $y_i \in R$ and let $A = \{(r_1, \dots, r_n) \in R^n \mid x_1r_1 + \cdots + x_nr_n = 0\}$.

(a) Show $R^n \cong A \oplus R$:

Define the map $\varphi: R^n \to R$, $(r_1, \dots, r_n) \mapsto x_1r_1 + \cdots + x_nr_n$, hence $\ker\varphi = A$.

Furthermore, $r = r \cdot 1 = r(x_1y_1 + \cdots + x_ny_n) = r\varphi(y_1, \dots, y_n)$

$= \varphi(ry_1, \dots, ry_n)$, hence φ surj.

Therefore, by First Isom Thm, $R^n/A \cong R$

Now consider the short exact sequence $0 \to \underset{A}{\ker\varphi} \to R^n \to R \to 0$

This sequence splits because R is a free R-module, hence $R^n \cong A \oplus R$.

(b) A has n generators as an R-module

A has n gen as R-mod $\iff \exists$ surj. hom $\Psi: R[t_1, \dots, t_n] \twoheadrightarrow A$

Since R^n finitely-generated with n generators, we already have $\Psi: R[t_1, \dots, t_n] \twoheadrightarrow R^n$. Let $\pi_A: A \oplus R \cong R^n \twoheadrightarrow A$ be the projection map.

Then: $R[t_1, \dots, t_n] \xrightarrow{\Psi} R^n \cong A \oplus R \xrightarrow{\pi_A} A$, hence $\pi_A \circ \Psi$ surjective onto A,

hence A has n gen. as an R-module.

(c) Show when $R = F[x]$, F field, then A_R is free of rank $n-1$.

$R = F[x] \Rightarrow R$ a PID, hence apply the Fund Thm of Modules / PID, hence $A = R^k \oplus A_t$ ← torsion part, but $R^n \cong A \oplus R \cong R^k \oplus A_t \oplus R$, hence $A_t = 0$ since R^n is free, hence $A = R^k$, hence A free.

But $R^n \cong A \oplus R = R^k \oplus R = R^{k+1} \Rightarrow k = n-1 \rightarrow \operatorname{rk} A = n-1$

---

(5) $R = \mathbb{C}[x_1, \dots, x_n]$, $I \subsetneq R$ ideal. If $A \in M_k(R)$ & $A(\alpha) = 0$ for all $\alpha \in \operatorname{Var}(I)$, show that for some $N > 0$, $A^N \in M_k(I)$.

$A \in M_k(R)$, so $A = [a_{ij}]$ with $a_{ij}(\alpha) = 0 \ \forall \alpha \in \operatorname{Var}(I)$

$\Rightarrow a_{ij} \in \operatorname{Id}(\operatorname{Var}(I)) = \sqrt{I}$

Hence, for all a_{ij}, $\exists t$ such that $a_{ij}^t \in I$.

Since $R = \mathbb{C}[x_1, \dots, x_n]$ is noetherian by the Hilbert Basis Theorem, every ideal in R is finitely-generated, Hence $\sqrt{I}$ is finitely-gen.

$\Rightarrow \sqrt{I} = \langle r_1, \dots, r_\ell \rangle$, and so $a_{ij} \in \sqrt{I} \Rightarrow a_{ij} = \sum_{s=1}^{\ell} c_s r_s$

Each r_s has m_s such that $r_s^{m_s} \in I$, so let $m = \max_s(m_s)$, and so $r_s^m \in I$ for all $s = 1, \dots, \ell$.

Now choose $N = \ell m$ s.t. $(\sum c_s r_s)^N$ each term has total degree $\geq \ell m$ (hence so each term has an r_s^m, hence $\in I$).

$A^{Nk^2} = [a_{ij}]^{Nk^2}$ will have entries whose sum terms will be of total degree $\geq Nk^2$, hence each will have an $a_{ij}^N \in I$, hence all entries are in I, Hence $A^{Nk^2} \in M_k(I)$

(6) R artinian $\mathbb{C}$-algebra:

Show: $\exists\, m \geq 1$ s.t. of $x \in R$ s.t. $x^k = 0$ for some $k \geq 1$, then $x^m = 0$.

R artinian $\Rightarrow$ $J(R)$ nilpotent

case R semisimple: By Art-Wedderburn, $R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$, where the D_i are division rings s.t. $D_i \subseteq M_{n_i}(D_i)$, hence each D_i is also an artinian $\mathbb{C}$-algebra.

Suppose $x \in M_{n_i}(D_i) = R_i$ is a nilpotent element with $x^k = 0$. Recall that, as an additive groups, $M_{n_i}(D_i) \cong C_1 \oplus \cdots \oplus C_{n_i}$, where the C_j are the column ideals.

Ideals are additive subgroups, hence they are also direct sums of the C_j's; so then a chain of ideals with proper containments $R_i \supsetneq I_1 \supsetneq I_2 \supsetneq \cdots$ can have length at most n_i since R_i is artinian.

Now consider the chain of ideals $R_i \supseteq R_i x \supseteq R_i x^2 \supseteq \cdots \supseteq R_i x^k = 0$, hence $k \leq n_i$. Therefore, $x^{n_i} = 0$.

Now choose nilpotent elt. $x \in R$. Then $x = (x_1, \ldots, x_k)$ with $x_i \in M_{n_i}(D_i)$ and $x^a = (x_1^a, \ldots, x_k^a) = 0$ for some $a > 0$; therefore the x_i are nilpotent in $M_{n_i}(D_i)$, hence $x_i^{n_i} = 0$, so let $n = \max_i \{n_i\}$, hence $x_i^n = 0 \ \forall i$.

General case: Consider $R/J(R)$. R artinian, hence $R/J(R)$ artinian. $R/J(R)$ Jacobson s.s. & artinian $\Rightarrow$ semisimple, hence by the semisimple case there is m s.t. for elements $x \in R$ with $x^k \in J(R)$ for some k, $x^m \in J(R)$.

Now, since $J(R)$ nilpotent, $J(R)^l = 0$, hence $x^{ml} = 0$ for any nilpotent element (since nilp $\Rightarrow x^k = 0 \in J(R)$ some k)