ALGEBRA QUALIFYING EXAM FALL 2011

Work all of the problems. Justify the statements in your solutions by reference to specific results, as appropriate. Partial credit is awarded for partial solutions. The set of integers is $\boldsymbol{Z}$, the set of rational numbers is $\boldsymbol{Q}$, and set of the complex numbers is $\boldsymbol{C}$.

1. Let I and J be ideals of $R = \boldsymbol{C}[x_1, x_2, \ldots, x_n]$ that define the same variety of $\boldsymbol{C}^n$. Show that for any $x \in (I + J)/I$ there is $m = m(x) > 0$ with $x^m = 0_{R/I}$. Show there is an integer $M > 0$ so that for any $y_1, y_2, \ldots, y_M \in (I + J)/I$, $y_1 y_2 \cdots y_m = 0_{R/I}$.

2. If $K \subseteq L$ are finite fields with $|K| = p^n$ and $[L : K] = m$ then show that for each $1 \leq t < nm$, any $a \in L - K$ has a p^t–th root in L. When $m = 3$, show that every $b \in K$ has a cube root in L.

3. Let F be an algebraically closed field and A an F-algebra with $\dim_F A = n$. If every element of A is either nilpotent or invertible, show that the set of nilpotent elements of A is an ideal M of A, that M is the unique maximal ideal of A, and that $\dim_F M = n - 1$.

4. Let M be a finitely generated $F[x]$ module, for F a field.
   i) Show that if $f(x)m = 0$ for $f(x) \neq 0$ forces $m = 0$, then M is a projective $F[x]$ module.
   ii) If H is an $F[x]$ submodule of M show that $M = H \oplus K$ for a submodule K of M if and only if: $f(x)m \in H$ for $f(x) \neq 0$ implies that $m \in H$.

5. Up to isomorphism, describe the possible structures of any group of order $987 = 3 \cdot 7 \cdot 47$.

6. Let $R = \boldsymbol{Z}[x_1, x_2, \ldots x_n, \ldots]$ and let $\{f_i(X) \mid i \geq 1\} \subseteq R$ satisfy $f_1(X)R \subseteq f_2(X)R \subseteq \cdots \subseteq f_i(X)R \subseteq \cdots$. Show $f_s(X)R = f_m(X)R$ for some m and all $s \geq m$.

7. Let U be the set of all n-th roots of unity in $\boldsymbol{C}$, for all $n \geq 3$, and set $F = \boldsymbol{Q}(U)$. For primes $p_1 < \cdots < p_k$ and nonzero $a_1, \ldots, a_k \in \boldsymbol{Q}$, set $M = F(a_1^{1/p_1}, \ldots, a_k^{1/p_k}) \subseteq \boldsymbol{C}$. Show that M is Galois over F with a cyclic Galois group. For any subfield $F \subseteq L \subseteq M$, show that there is a subset T of $\{a_j^{1/p_j}\}$ so that $L = F(T)$.

Algebra – Fall 2011:

① $I, J \subseteq R = \mathbb{C}[x_1, \dots, x_n]$ ideals such that $Var(I) = Var(J)$.

(a) Show that for any $x \in (I+J)/I$, $\exists\, m(x) > 0$ w/ $x^m = 0_{R/I}$.

$Var(I) = Var(J) \Rightarrow Id(Var(I)) = Id(Var(J)) \Rightarrow \sqrt{I} = \sqrt{J} \supseteq J$, hence $J \subseteq \sqrt{I}$ and for each $j \in J$, $\exists\, k(j) = k$ s.t. $j^k \in I$.

Now choose $x \in I+J \Rightarrow x = i + j$ for $i \in I$, $j \in J$.

Then $x^k = (i+j)^k = \underset{\in I}{i^k} + (\text{cross terms}) + \underset{\in I}{j^k} \Rightarrow x^k \in I$.

since each has such of i and $i \in I$ an ideal.

So then for each $x \in J+J$, $\exists\, m(x) = m$ with $x^m \in I$,

hence for $x \in (I+J)/I$, $\exists\, m(x) = m$ with $x^m = 0_{R/I}$.

(b) Show that there is an integer $M > 0$ s.t. for any $y_1, \dots, y_M \in (I+J)/I$, $y_1 \cdots y_M = 0_{R/I}$.

$R = \mathbb{C}[x_1, \dots, x_n]$ noetherian by Hilbert basis, hence $I+J = \langle r_1, \dots, r_k \rangle$

By the previous part, $\exists\, m_i > 0$ such that $r_i^{m_i} \in I$ for each $i = 1, \dots, k$.

Let $m = \max_i \{m_i\}$; then $r_i^m \in I \ \forall i$.

Now choose $y_1, \dots, y_M \in I+J$; then $y_j = \sum_{i=1}^{k} a_i^{(j)} r_i$

and let $M = mk$.

Then $\prod_{j=1}^{M} y_j = \prod_{j=1}^{mk} \left(\sum_{i=1}^{k} a_i^{(j)} r_i \right)$ is a product of mk linear combinations of the k elements $\{r_i\}$, hence the total degree in the r_i of each summand of this product must be mk. Since there are only k r_i, it must be that each summand has an r_i^m for some i, hence summand has an $r_i^m \in I$, hence entire summand is in I, hence $\prod_{j=1}^{M} y_j \in I$ since all summands are. Therefore, $\prod y_j = 0_{R/I}$.

(2) $K \subseteq L$ finite fields with $|K| = p^n$ & $[L:K] = m$, then show that for each $1 \le t < nm$, any $a \in L|K$ has a p^t-th root in L.

(a) Let $|K| = p^n = q$. Since $|L| = p^k$ some $k \in \mathbb{N}$, $n \mid k \Rightarrow k = mn$ $\Rightarrow |L| = q^m$, and $\therefore [L:K] = m$. Now consider the Frobenius automorphism $\sigma : \underset{x \mapsto x^p}{L \to L}$ and recall $\langle \sigma \rangle = \mathrm{Gal}(L/\mathbb{F}_p) = \mathbb{Z}_{mn}$, hence every automorphism fixing $\mathbb{F}_p$ is given by σ^t, $t = 1, \dots, mn$. Now consider $\sigma^t : \underset{\langle a \rangle \mapsto a^{p^t}}{L^\times \to L^\times}$; clearly this is a group automorphism since $\sigma^t \in \mathrm{Gal}(L/\mathbb{F}_p) \subseteq \mathrm{Aut}(L)$, hence it is surjective, hence $\sigma^t : \underset{a \mapsto a^{p^t}}{L \to L}$ surjective on L, hence for $a \in L$, $\exists\, b \in L$ s.t. $a = \sigma^t(b) = b^{p^t}$.

(b) For $[L:K] = 3$, show every $b \in K$ has a cube root in L.

Now $|L| = q^3$, $|K| = q$, hence $|L^\times| = q^3 - 1$ & $|K^\times| = q - 1$ and both are cyclic. We want to show now that $\varphi : \underset{x \mapsto x^3}{L^\times \to L^\times}$ has $K^\times \le \varphi(L^\times)$. Let $L^\times \cong \langle a \rangle$; then $\varphi(a) = a^3$ will generate $L^\times$ if $3 \nmid (q^3 - 1)$, and hence statement is true. Now suppose $3 \mid q^3 - 1$; then $|\varphi(L^\times)| = \frac{q^3-1}{3}$ cyclic, hence if $(q-1) \mid \frac{q^3-1}{3}$ then $K^\times \le \varphi(L^\times)$. See that $3 \mid (q^3 - 1) = (q-1)(q^2+q+1)$, hence $3 \mid (q-1)$ or $3 \mid q^2+q+1$ since 3 prime:

- Case $3 \mid q^2+q+1$: then $\left(\frac{q^2+q+1}{3}\right)$ an integer & thus $\frac{q^3-1}{3} = \left(\frac{q^2+q+1}{3}\right)(q-1)$, hence $(q-1) \mid \frac{q^3-1}{3} \Rightarrow K^\times \le \varphi(L^\times)$ ✓
- Case $3 \mid (q-1)$: $q \equiv 1 \pmod 3 \Rightarrow q^3 \equiv 1 \pmod 3 \Rightarrow q^2+q \equiv 2 \pmod 3 \Rightarrow q^2+q+1 \equiv 3 \pmod 3$ $\Rightarrow q^2+q+1 \equiv 0 \pmod 3 \Rightarrow 3 \mid q^2+q+1 \Rightarrow$ Case 1 $\Rightarrow K^\times \le \varphi(L^\times)$ ✓

③ F algebraically closed field and A an F-algebra with $\dim_F A = n$ and every element $a \in A$ is either nilpotent or invertible.

Show that the set of nilpotent elements in A is an ideal of A and that it is a unique maximal ideal, and

Let N be the set of nilpotent elements in A. and choose $a \in N$ and $b \in A$. Suppose $ab \notin N$; then ab has an inverse $u \in A$ so that $abu = 1 \Rightarrow (a)(bu) = 1 \Rightarrow a$ invertible, contradiction since a nilpotent, so $ab \in N$.

Now let $a, b \in N$ and suppose $a+b \notin N$. Then $a+b$ is invertible, hence $\exists u$ s.t. $1 = (a+b)u = au + bu$. By the previous paragraph, $au, bu \in N$, hence nilpotent. Recall that if $x \in A$ is nilpotent, then $1-x$ is a unit, $x^k = 0$ for some k and thus $(1-x)(1+x+\cdots+x^{k-1})$

$= 1 + x + \cdots + x^{k-1} - x(1+x+\cdots+x^{k-1}) = 1 + x + \cdots + x^{k-1} - (x + \cdots + x^{k-1} + x^k)$

$= 1$

Hence $1-x$ a unit, and therefore, $bu = 1 - au$ is a unit, which is a contradiction since $bu \in N$; therefore $a+b \in N$

Hence N is an ideal in A.

Case A semi-simple: By Artin-Wedderburn $A \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$

A is an F-algebra, hence so are the D_i's. Now choose $x \in D_i$; clearly $F(x) \subseteq D_i$, hence $F(x)$ is fin dim'l F-v.s., hence $F(x)/F$ finite extension, hence algebraic, hence $F(x) = F$ since F alg. closed, hence $x \in F$, hence $D_i \subseteq F \Rightarrow D_i = F$.

So $A \cong M_{n_1}(F) \oplus \cdots \oplus M_{n_k}(F)$

But A has only nilpotent or invertible elts; direct sum has non-nilpotent zero divisors so $k=1$ and $A \cong M_n(F)$.

Matrix ring has noninvertible elts not nilpotent, hence $n=1$, and $A \cong F$.

So A is a field and thus $N=(0)$ (hence $\dim_k N = 0 = \dim_k^{''} A - 1$)

General case: Consider $A/J(A)$. A is artinian, hence so is $A/J(A)$ & $J(A)$ is nilpotent. $A/J(A)$ also Jacobson semisimple, hence semisimple, so back to semisimple case, namely $A/J(A) \cong F$. and

Now, since $J(A)$ nilpotent, $J(A) \subseteq N$ and thus $N/J(A)$ are the nilpotent elts of $A/J(A)$; we just showed this a field, hence $N/J(A) \cong 0 \Rightarrow N \cong J(A)$

$\Rightarrow$ $\Rightarrow A/N \cong F$, hence $\dim_k N = n-1$

Now, since $A \setminus N$ = units of A, we have that all ideals of A must consist of elements in N since if a unit is in an ideal then it equals the entire ring. Therefore the ideal N of all the nonunits is unique maximal ideal (since if $N \subsetneq I \subsetneq A$ then I has a unit, hence $I = A$)

④ M fin-gen F[x] module for F field

(i) Show that if $f(x)m=0$ for $f(x)\neq 0$ forces $m=0$, then M is a projective F[x]-module.

Let $F[x]=R$; now apply Fund thm of mod/PID to get: $M=R^k \oplus M_t$; Now, for $m\in M$, $m=s+t$ and for $f(x)\in R$ nonzero, $f(x)m=f(x)s+f(x)t=0 \Rightarrow m=0$ clearly implies $s=0$, but a nontrivial torsion element could exist with this property, hence $M_t=0$, hence M free, hence M projective

(ii) $H\subseteq M$ an F[x]-submodule; show that: $M=H\oplus K$ for submod $K\subseteq M \iff f(x)m\in H$ for $f(x)\neq 0$ implies $m\in H$

($\Rightarrow$) $M=H\oplus K$, hence $K\cong M/H$, and suppose $f(x)m=0\in M/H$. But M is free, hence by Fund thm mod/PID, any submod is torsion free, hence K torsion free.

Therefore, $f(x)m=0$ in $K \Rightarrow m=0$ in $K \to m\in H$.

($\Leftarrow$) suppose for $f(x)\neq 0$, $f(x)m\in H \Rightarrow m\in H$.; this is the same as saying $f(x)m=0$ in $M/H \Rightarrow m=0$ in M/H, hence M/H is torsion-free $\neq$ obviously finitely gen over PID, hence M/H free

Then we have short exact sequence

$$0 \to H \to M \to M/H \cong F[x]^n \to 0$$

and since M/H free, it splits, hence $M\cong H\oplus F[x]^n$, hence H direct sum of F[x]-module.

(5) $|G| = 987 = 3 \cdot 7 \cdot 47$.

Sylow: $r_{47} = 1 \pmod{47}$ & $r_{47} \mid 3 \cdot 7 \Rightarrow r_{47} = 1, \cancel{3}, \cancel{7}, \cancel{21} \Rightarrow$ N Sylow 47-sg is normal

$r_7 = 1 \pmod 7$ & $r_7 \mid 3 \cdot 47 \Rightarrow r_7 = 1, \cancel{47}, 3 \cdot 47$

$r_3 = 1 \pmod 3$ & $r_3 \mid 7 \cdot 47 \Rightarrow r_3 = 1, \cancel{7}, \cancel{47}, \cancel{7 \cdot 47}$

So $N \trianglelefteq G$ the Sylow 47-subgroup is normal.

Now choose Q to be a Sylow 7-subgroup and we have NQ subgroup index 3. Consider repn on cosets $\varphi: G \to S_3$, $NQ \subseteq \ker\varphi$.

See that $|G/\ker\varphi| \mid 3!$ & $|G/\ker\varphi| \mid |G| = 3 \cdot 7 \cdot 47$

$\Rightarrow |G/\ker\varphi| \mid \gcd(3!, 3 \cdot 7 \cdot 47) = 3 \Rightarrow |G/\ker\varphi| = 3 \Rightarrow |\ker\varphi| = 7 \cdot 47 = |NQ|$

$\Rightarrow \ker\varphi = NQ$, hence normal.

Now choose S a Sylow 3-subgroup.

$S \cap NQ = 1$ since orders coprime, hence $SNQ \cong G$, hence $G \cong S \ltimes NQ$, so we have hom $\varphi: S \to \mathrm{Aut}(NQ) \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{46}$.
$s \longmapsto \sigma_s(n) = snS^{-1}$

The image must have order 1 or 3, so:

order 1: abelian, hence $\boxed{G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{47}}$

order 3: want $\sigma_s^3 = \mathrm{id}$, See that $\mathrm{Aut}(NQ) \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{46}$.

and $6 = 2 \cdot 3$ & $46 = 2 \cdot 23$, hence for $\mathbb{Z}_6 \oplus \mathbb{Z}_{46} \cong \langle a \rangle \oplus \langle b \rangle$, the order 3 elts are $(a^2, 1)$ & $(a^4, 1)$

So $\theta_1(\alpha, \beta) = (\alpha^2, \beta)$ (and $\theta_1^2(\alpha, \beta) = (\alpha^4, \beta)$)

So, suppose $\sigma_s(\alpha, \beta) = \theta_1(\alpha, \beta) = (\alpha^2, \beta) \Rightarrow$

Let $\mathbb{Z}_7 \oplus \mathbb{Z}_{47} \cong \langle \alpha \rangle \oplus \langle \beta \rangle$ and we want $k^3 \equiv 1 \pmod 7$

$\Rightarrow (k-1)(k^2+k+1) \equiv 0 \pmod 7$

$\Rightarrow k^2 + k \equiv -1 \pmod 7$

$\Rightarrow k(k+1) \equiv 6 \pmod 7 \Rightarrow k = 2$

$\boxed{G \cong \langle s, \alpha, \beta : s^3 = \alpha^7 = \beta^{47} = 1, \; s\alpha s^{-1} = \alpha^2, \; s\beta s^{-1} = \beta \rangle}$

(note $s\alpha^2 s^{-1} = \alpha^4 \Rightarrow s\alpha^4 s^{-1} = \alpha$ for θ_1^2)

(6) $R = \mathbb{Z}[x_1, \dots, x_n, \dots]$ and let $\{f_i : i \geq 1\} \subseteq R$ satisfy the chain $(f_1) \subseteq (f_2) \subseteq \cdots \subseteq (f_t) \subseteq \cdots$

Show that the chain terminates for some M...

$f_1 \in R$ polynomial, hence in finite number of variables, hence for some m, $f_1 \in \mathbb{Z}[x_1, \dots, x_m] := R_1 \subseteq R$.

Then $(f_1) \subseteq (f_2) \Rightarrow \exists g \in R$ such that $gf_2 = f_1 \in R_1$.

Suppose $f_2 \notin R_1$; R_1 gf_2 UFD, so $f_1 = gf_2 = p_1 \cdots p_k$ in R_1.

Now since $f_2 \notin R_1$, $f_2 \in \mathbb{Z}[x_1, \dots, x_m, \dots, x_\ell]$, but the p_i are still primes in here, and $\mathbb{Z}[x_1, \dots, x_\ell]$ is also a UFD, hence $gf_2 = p_1 \cdots p_k$ unique factorization in here, hence some subset of the $\{p_i\}$ is the factorization of f_2 (since UFD), hence f_2 a product of $p_i \in R_1$, hence contradiction $\Rightarrow f_2 \in R_1$

Repeating the same procedure we get $f_1, f_2, \dots \in R_1$, hence $f_1 R_1 \subseteq f_2 R_1 \subseteq \cdots$ as ideals in R_1; but R_1 is noeth. by Hilbert basis, hence $f_1 R_1 \subseteq f_2 R_1 \subseteq \cdots \subseteq f_M R_1 = f_{M+1} R_1$ for some M, and note that if $f_M R_1 = f_{M+1} R_1$, we also have that $f_M R = f_{M+1} R$, hence $(f_1) \subseteq (f_2) \subseteq \cdots \subseteq (f_M) = (f_{M+1})$

(7) U = all roots of unity in $\mathbb{C}$, $F = \mathbb{Q}(U)$

For primes $p_1 < \cdots < p_k$ and nonzero $q_1, \ldots, q_k \in \mathbb{Q}$, let $M = F(\sqrt[p_1]{q_1}, \ldots, \sqrt[p_k]{q_k}) \subseteq \mathbb{C}$.

Show that M/F Galois with cyclic Galois group

Each $\sqrt[p_i]{q_i}$ has minimal polynomial $x^{p_i} - q_i \in \mathbb{Q}[x]$, each of which have roots $\omega_i^j \sqrt[p_i]{q_i}$ where ω_i is a p_i^{th} root of unity and $1 \le j \le p_i$, hence each of $x^{p_i} - q_i$ splits in M since $\omega_i \in M$ for all i. Since distinct primes, note that $F(\sqrt[p_i]{q_i}) \neq F(\sqrt[p_j]{q_j})$, hence we have $\sqrt[p_i]{q_i}$ has the same min poly over $F(\sqrt[p_1]{q_1}, \ldots, \sqrt[p_{i-1}]{q_{i-1}})$, hence adjoining $\sqrt[p_i]{q_i}$ results in a p_i-degree extension:

$$M = F(\sqrt[p_1]{q_1}, \ldots, \sqrt[p_k]{q_k})$$
$$\vdots \quad \Big) p_k$$
$$F(\sqrt[p_1]{q_1}, \ldots, \sqrt[p_{k-1}]{q_{k-1}}) \quad \Big) p_{k-1}$$
$$\vdots$$
$$F(\sqrt[p_1]{q_1}) \quad \Big) p_2$$
$$F \quad \Big) p_1$$

$\Rightarrow$ By tower law, $[M/F] = \prod_{i=1}^{k} p_i$.

Since normal, separable extension & finite degree $\Rightarrow$ Galois.

Clearly by same logic all subfields are Galois, hence there are normal subgroups of every index; in particular, every Sylow p-group is normal, hence unique, hence

$$\mathrm{Gal}(M/F) \cong \mathbb{Z}_{p_1} \oplus \cdots \oplus \mathbb{Z}_{p_k} \cong \mathbb{Z}_{p_1 \cdots p_k}$$

so cyclic.