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 $1 \le t < nm$, 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 $\{f_i(X) \mid i \ge 1\} \subseteq R$ 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 $s \ge m$.

7. Let U be the set of all n-th roots of unity in $\boldsymbol{C}$, for all $n \ge 3$, 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 ideals of $R = \mathbb{C}[x_1, x_2, \ldots, x_n]$

s.t. $V(I) = V(J) \subset \mathbb{C}^n$.

Show for any $x \in (I+J)/I$ there is

$m \equiv m(x) > 0$ s.t. $x^m = 0 \in R/I$.

Show there is $M > 0$ s.t. for all $y_1, y_2, \ldots, y_M \in$

$\in (I+J)/I$, $y_1 y_2 \cdots y_M = 0 \in R/I$.

---

solution

Let $x \equiv \overline{f(x)}$, $f(x) \in I + J$.

So $V(f(x)) \supset V(I+J) = V(I) \cap V(J) = V(I)$.

So $f(x) \in \sqrt{(f(x))} = \mathcal{I}V(f(x)) \subset \mathcal{I}V(I) = \sqrt{I}$.

So $\exists m$ s.t. $f(x)^m \in I \Longrightarrow x^m = 0 \in R/I$.

Since $\mathbb{C}[x_1, \ldots, x_n]$ is Noetherian, choose finitely many generators $a_1, \ldots, a_n$ for J. we want to show if $f_1, \ldots, f_M \in I+J$ for some M, then $f_1 \cdots f_M \in I$. Observe if we

write $f_1 = f_1^I + f_1^J, \ldots, f_M = f_M^I + f_M^J$,

then $(f_1^I + f_1^J) \cdots (f_M^I + f_M^J) \in I$ iff

$f_1^J \cdots f_M^J \in I$; so we may assume

the $f_1, \ldots, f_M \in J$.

Recall $J = (a_1, \ldots, a_n)$. Define M as

follows: choose m_j s.t. $a_i^{m_i} \in I$, $i = 1, \ldots, n$, and

set $M := n \max_i \{m_i\}$.

If $f_1 = b_{11} a_1 + \cdots + b_{1n} a_n, \ldots,$

$f_M = b_{M1} a_1 + \cdots + b_{Mn} a_n$, then

$$f_1 \cdots f_M = \left(\sum_{i_1=1}^{n} b_{1 i_1} a_{i_1} \right) \cdots \left(\sum_{i_M=1}^{n} b_{M i_M} a_{i_M} \right)$$

$$= \sum_{i_1, \ldots, i_M = 1}^{n} \left(b_{1 i_1} \cdots b_{M i_M} \right) a_{i_1} \cdots a_{i_M}.$$

Each monomial $a_{i_1} \cdots a_{i_M}$ in this homogeneous polynomial has to have some j s.t. a_{i_j} has power $\geq \max_i \{m_i\}$; otherwise, the monomial has deg $< n \cdot \max_i \{m_i\} = M$, which is impossible. So as $a_{i_j}^{m_j} \in I$, each monomial $a_{i_1} \cdots a_{i_M} \in I$, and we are done. $\square$

(2) Let $K \subset L$ finite fields w/ $|K| = p^n$ and $[L : K] = m$. Show for each $1 \leq t \leq nm$ that any $a \in L - K$ has a p^t-th root in L. When $m = 3$, show every $b \in K$ has a cube root in L.

---

solution

For the first statement, it appears the result is true for any $a \in L$, not just $a \in L - K$:

Fix $1 \leq t \leq nm$. By definition L is the splitting field over F_p of $X^{p^{nm}} - X$. So if $a \in L$ then $a^{p^{nm}} = a$. writing $p^{nm} = p^t p^{nm-t}$ we have $a = a^{p^{nm}} = a^{p^t p^{nm-t}} = (a^{p^{nm-t}})^{p^t} \equiv b^{p^t}$; so b is a p^t-th root of a in L, as desired.

Next, we want to show if $a \in F_{p^n}$ then there is $b \in F_{p^{nm}}$ s.t. $b^3 = a$. we know $a^{p^{3n}} = a$ and $a^{p^n} = a$.

If $p^{3n} \equiv 0 \pmod 3$ then we are done, since

$a = a^{p^{3n}} = a^{3X} = (a^X)^3 =: b^3$. Using $a^{p^n} = a$, we can say

$a^{p^{3n}} = a^{p^{3n}-(p^n-1)}$. We split into cases. If $p^{3n} \equiv 1 \pmod 3$

and if $p^n - 1 \equiv 1$ or $2 \pmod 3$, then

$a = a^{p^{3n}} = a^{p^{3n}-(p^n-1)} =: b^3$ or $a = a^{p^{3n}} = a^{p^{3n}-2(p^n-1)} =: b^3$, respectively;

and similarly if $p^{3n} \equiv 2 \pmod 3$. (Note that $p^{3n} > 2(p^n-1)$.)

However, if $p^n - 1 \equiv 0 \pmod 3$, i.e. $3 \mid p^n - 1$,

then this method fails, and we must resort to Galois theory.

Lemma

Let q be a prime. If F_{p^n} contains a primitive q^{th} root of unity, then every $a \in F_{p^n}$ has a q^{th} root b in $F_{p^{nq}}$.

Proof (lemma): If there exists a q^{th} root b of a in F_{p^n}, then we are done. Otherwise, choose such a b in $\overline{F_{p^n}}$ and let $\zeta \in F_{p^n}$ be a q^{th} root of unity. Consider the extension $F_{p^n} \subset F_{p^n}(b)$, which is the splitting field of the poly $f(X) = X^q - a \in F_{p^n}[X]$, since the roots of $f(X)$ are $b\zeta^i$ $(i = 0, 1, \ldots, q-1)$ and $\zeta \in F_{p^n}$. Since the extension is simple, its degree over F_{p^n} is $\leq q$.

In particular, since the extension is Galois, being a splitting extension of a separable polynomial, $|Gal(F_{p^n}(b)/F_{p^n})| = [F_{p^n}(b) : F_{p^n}] \leq q$ and so every elt of the Galois group has order $\leq q$.

Now, let $\varphi \neq e$ be an elt of the Galois group. Since the ext is simple, φ sends $b \mapsto b\zeta^k$ for some $k = 1, 2, \ldots, q-1$ ($b \not\mapsto b$ since $\varphi \neq e$). Since $\zeta \in F_{p^n}$, φ fixes ζ, so we gather $b \xmapsto{\varphi} b\zeta^k \xmapsto{\varphi} b\zeta^{2k} \mapsto \cdots$

Since q is prime and ζ is a primitive q^{th} root of unity, we have $(k, q) = 1$ and so $|\varphi| = q$. We conclude the Galois group has order q and is in fact cyclic. Hence, $[F_{p^n}(b) : F_{p^n}] = q$.

And $F_{p^{nq}}$ is the unique ext of degree q over F_{p^n}. We conclude $b \in F_{p^{nq}}(b) \cong F_{p^{nq}}$ is the desired q^{th} root of a, proving the lemma. $\square$

Recall we are in the setting $3 \mid p^n - 1$. Recall that the group of units $(F_{p^n})^\times$ has order $p^n - 1$ and is in fact cyclic. Either by Cauchy's theorem, or by the theory of cyclic groups, we gather F_{p^n} has a primitive 3^{rd} root of unity. By the lemma, we are done. $\square$

(3) F alg closed. A is an F-alg w/ $\dim_F A = n$. Assume every elt of A is either a nilpotent or invertible. Show $M = \{$ nilpotent elts $\}$ is an ideal, the unique maximal ideal, and $\dim_F M = n-1$.

---

solution

Recall a nil ideal is an ideal s.t. every elt is nilpotent (not necessarily w/ a uniform exponent). If such a uniform exponent exists, then the ideal is called a nilpotent ideal.

Let $x \in A$ be nilpotent. Then Ax is a left ideal. Moreover, Ax is a left nil ideal: If ax were not nilpotent, then by assumption it is invertible. Let k be minimal s.t. $x^k = 0$. Then there exists $y \in A$ s.t. $yax = 1$. Multiplying on the right by x^{k-1} we obtain $0 = x^{k-1}$ $\Rightarrow\Leftarrow$. So Ax is a left nil ideal.

It is a theorem that the Jacobson radical J

contains every left (or right) nil ideal.

Therefore $x \in J$. So $M \subset J$. It is also a theorem that J is a 2-sided ideal. Therefore, all invertible elts lie outside J. So $M = J$ is a 2-sided ideal, as desired.

The same logic says any 2-sided ideal only contains nilpotent elts, and so must be contained in $J = M$. Thus, M is the unique maximal ideal in A.

Now consider A/M which contains only invertible elts (except 0). In particular, A/M is a f.d. integral algebra over F. So every elt α of A/M is the root of a poly in $F[x]$. Since A/M is integral, the number of roots of f in A/M is at most $\deg f$. Since F is alg closed, F contains these $\deg f$ roots. So $\alpha \in F$. That is $A/M = F$ is 1-dim. We conclude $\dim_F M = n-1$. □

(4) (This problem is a little buggy.)

M f.g. $F[x]$-module, F a field.

(a) Show if $[f(x)m = 0, \forall f(x) \neq 0 \Longrightarrow m = 0]$

then M is a projective $F[x]$-module.

(b) If H is an $F[x]$-submodule of M,

show $[M = H \oplus K$ for a submodule K of $M]$ $\Longleftrightarrow$ (**)

$[f(x)m \in H$, for some $\forall f(x) \neq 0 \Longrightarrow m \in H]$.

(*) Surely it is not meant 'for all $f(x) \neq 0$', since this is always False taking $f(x)^{-1}$ so $[_ \Rightarrow _]$ is always True, so [If True, then M is projective] is False, as not all f.g. $F[x]$-modules are project (those w/ torsion).

solution to (a) (as changed above)

' for all $f(x)$, $\deg f \geq p$! (**) The converse is false if we keep 'for some $f(x) \neq 0$'!

$$M \cong \frac{F[x]}{(d_1(x))} \oplus \cdots \oplus \frac{F[x]}{(d_n(x))} \oplus F[x]^r$$

If there is a torsion part, then

$d_1(x) \neq 0$ and $d_1(x) \cdot (1, 0, \ldots, 0, \vec{0}) = \neq 0 \in M$. So there cannot be a torsion part. So M is a free $F[x]$-module. So M is a projective $F[x]$-module. $\square$.

($\uparrow n$, $\neq 0$)

$d_1(X) \neq 0$ and $d_1(X) \cdot (1, 0, \ldots, \underset{\uparrow}{0}, \vec{0}) = 0 \in M$.
$\quad\quad\quad

(5) Describe groups of order $987 = 3 \cdot 7 \cdot 47$.

Solution

$\langle x \rangle = P$ Sylow 3-s.g. $\quad \langle y \rangle = Q$ Sylow 7-s.g. $\quad \langle z \rangle = R$ Sylow 47-s.g.

$n_3 = 1, 7, \cancel{47}, \cancel{7 \cdot 47}$ $\quad n_7 = 1, \cancel{7}, \cancel{47}, 3 \cdot 47$ $\quad n_{47} = 1, \cancel{3}, \cancel{7}, \cancel{21}$

mod 3: $1, 1, 2, 2$ $\quad$ mod 7: $1, 3, 5, 1$

$R \trianglelefteq G$. $[G : QR] = 3$ smallest prime $|[G]$

$\Rightarrow QR \trianglelefteq G$. $G \cong QR \rtimes_\varphi P$,

determined by $\varphi : C_3 \to \mathrm{Aut}(QR)$.

In QR, $n_7 = 1, \cancel{47}$, so $Q \trianglelefteq QR$, $R \trianglelefteq QR$.

So $QR \cong Q \times R$. So

$$\varphi : C_3 \to \mathrm{Aut}(C_7 \times C_{47}) \overset{\text{since } \gcd(7,47)=1}{\cong} C_6 \times C_{46}.$$

$C_3 = \langle x \rangle$ $\qquad$ $C_6 \times C_{46} = \langle \alpha \rangle \times \langle \beta \rangle$

Know $|\varphi(x)| \mid$ $\Rightarrow |\varphi(x)| = 1$ or 3. Since $3 \nmid 46$, the possibilities are: $x \mapsto (1,1), (\alpha^2, 1), (\alpha^4, 1)$.

Since the subgroups $\langle (\alpha^2, 1) \rangle = \langle (\alpha^4, 1) \rangle$ are the same, these two semidirect products coincide.

Observe $y \overset{\alpha}{\mapsto} y^3$ defines a generator α of $\mathrm{Aut}(C_7) \cong C_6$, because $y \mapsto y^3 \mapsto y^2 \mapsto y^6 \mapsto y^4 \mapsto y^5 \mapsto y$.

So the possible group structures are

$\langle x, y, z : x^3 = y^7 = z^{47} = 1,\ xy = y^3 x,\ xz = zx,\ yz = zy \rangle$

and $C_3 \times C_7 \times C_{47}$, two in total. $\square$

---

(6) $R = \mathbb{Z}[x_1, x_2, \ldots]$ and let $f_1(x), f_2(x), \ldots \in R$ satisfy $f_1(x)R \subset f_2(x)R \subset \cdots$. Show for some n we have $f_n(x)R = f_m(x)R$, $m \geq n$.

---

solution

R is a UFD since any $f(x) \in R$ is in a subring $\mathbb{Z}[x_{i_1}, \ldots, x_{i_k}]$, which is a UFD by Hilbert Basis Theorem + $\mathbb{Z}$ a UFD (Fundamental Theorem of Arithmetic).

$$R \text{ UFD} \iff \begin{cases} R \text{ satisfies ACCP} \\ \text{irred} \Rightarrow \text{prime} \end{cases}.$$

Since $f_1(x)R \subset f_2(x)R \subset \cdots$ is an ascending chain of principal ideals, it stabilizes. $\square$.

---

(7) Let $U = \{\zeta \in \mathbb{C} : \zeta \text{ } n^{\text{th}} \text{ root of unity}, n \geq 3\}$.

Let $F \equiv \mathbb{Q}(U)$. Let $p_1, \ldots, p_n$ be primes, s.t. $p_1 < \cdots < p_n$, and let (probably what was meant) $a_1, \ldots, a_n \in \mathbb{Q} - \{0\}$ nonzero, and set $L \equiv F\left(\sqrt[p_1]{a_1}, \ldots, \sqrt[p_n]{a_n}\right) \subset \mathbb{C}$. (1) $\longrightarrow$

Show that L is Galois over F w/ Cyclic Galois group. For any intermediate field $F \subset E \subset L$, show there are $a_{i_1}, \dots, a_{i_k}$ s.t. $E = F\left(\sqrt[p_{i_1}]{a_{i_1}}, \dots, \sqrt[p_{i_n}]{a_{i_n}}\right)$.

---

solution

To see L/F is Galois, we show it is the splitting field of the separable polynomial $f(X) = (X^{p_1} - a_1)(X^{p_2} - a_2) \cdots (X^{p_n} - a_n) \in F[X]$. The $\equiv f_1(X) \cdots f_n(X)$

roots of $f_i(X)$ are $\sqrt[p_i]{a_i}\, \zeta_{p_i}^j$ $(j = 0, 1, \dots, p_i - 1)$ if $a_i > 0$, $i^{\varepsilon} \sqrt[2]{|a_i|}$ $(\varepsilon = 0, 1)$ if $a_i < 0$ and $p_i = 2$, and $-\sqrt[p_i]{|a_i|}\, \zeta_{p_i}^j$ $(j = 0, 1, \dots, p_i - 1)$ if $a_i < 0$ and p_i odd. Since $p_1 < p_2 < \cdots < p_n$ we see $f(X)$ is separable. we also see L is indeed the splitting field of $f(X)$, since F contains all the roots of unity. So L/F is Galois.

(†) we may assume $|a_i| \neq 1$ and $|a_i|$ is not a p_i-th power, because otherwise we may absorb $\sqrt[p_i]{|a_i|}$ into F. (*)

To show the Galois group is cyclic

we show there is an elt of order $p_1 p_2 \cdots p_n$;
(see (*) below)

Since $[L:F] = [L:F(\alpha_1,\ldots,\alpha_n)][F(\alpha_1,\ldots,\alpha_n):F(\alpha_1,\ldots,\alpha_{n-1})]\cdots[F(\alpha_1):F]$

$\leq [F(\alpha_n):F][F(\alpha_{n-1}):F] \cdots [F(\alpha_1):F]$

$\leq p_n p_{n-1} \cdots p_1$

this shows the Galois group is generated by a single elt. The argument is essentially the same as in the proof of the lemma in Problem 2:

Any elt φ of the Galois group sends roots of $f_i(X)$ to roots of $f_i(X)$. So: $\underbrace{\pm \sqrt[p_i]{|a_i|}}_{\equiv \alpha_i} \overset{\varphi}{\mapsto} \underbrace{\pm \sqrt[p_i]{|a_i|}}_{\equiv \alpha_i} \zeta_{p_i}^{k_i}$ (1)

for some k_i for all i. However, not every such association (1) gives a well-defined φ, so we have to be a little careful. Our goal is to construct a φ s.t. (1) holds w/ $k_i \neq 0$ for all i; since all roots of unity are fixed by φ as they are in F, equation (1) implies $\alpha_i \overset{\varphi}{\mapsto} \alpha_i \zeta_{p_i}^{k_i} \overset{\varphi}{\mapsto} \alpha_i \zeta_{p_i}^{2k_i} \mapsto \cdots \mapsto \alpha_i$; since each p_i is prime and the p_i are mutually distinct, we conclude $|\varphi| = p_1 \cdots p_n$. It remains to construct φ satisfying (1) w/ $k_i \neq 0$ $\forall i$.

Let $m_i(\alpha_i)$ be the minimal poly of $F(\alpha_1,\ldots,\alpha_i)$ over $F(\alpha_1,\ldots,\alpha_{i-1})$. By our assumptions (†) and (*) we may assert that $\deg m_i(\alpha_i) > 1$. In particular, one of its roots is $\beta_i \equiv \alpha_i \zeta_{p_i}^{k_i}$ for some $k_i \neq 0$. Using the main theorem on simple extensions, $\alpha_i \mapsto \beta_i$ induces an automorphism φ_i of $F(\alpha_i)/F$, $\ldots$, $\alpha_i \mapsto \beta_i$ induces an auto φ_i of $F(\alpha_1,\ldots,\alpha_i)/F(\alpha_1,\ldots,\alpha_{i-1})$. Since φ_i fixes $F(\alpha_1,\ldots,\alpha_{i-1})$, this induces an auto φ of L/F defined

(*) Since we weren't asked show the extension is a specific degree, we may also assume $p_i\sqrt{|a_i|} \notin F(\sqrt[p_1]{|a_1|},\ldots,\sqrt[p_{i-1}]{|a_{i-1}|})$, otherwise we may again absorb the superfluous elt. This may be true as it is, but I am not sure and it is an unnecessary f... if true.

by $\varphi(x) = \begin{cases} x, & x \in F; \varphi_1(x), x \in F(\alpha_1) - F; \varphi_2(x), x \in F(\alpha_1,\alpha_2) - F(\alpha_1); \\ \cdots; \varphi_n(x), & x \in L - F(\alpha_1,\ldots,\alpha_{n-1}) \end{cases}$. With this def, φ satisfies (1) w/ $k_i \neq 0$ $\forall i$, so we conclude $Gal(L/F)$ is cyclic of degree $p_1 p_2 \cdots p_n$.

An intermediate field must be Galois, since the Galois group of L/F is cyclic and so every subgroup is normal. Therefore, every intermediate field has a unique image upon embedding into L. Therefore, we may characterize all intermediate fields by making explicit constructions.

For every $\{p_{i_1}, \ldots, p_{i_k}\}$, by copying the previous proof for L, we have that $F(p_{i_1},\ldots,p_{i_k})/F$ is a (Galois) intermediate field of L whose corresponding subgroup is cyclic of order $p_1 p_2 \cdots p_n / p_{i_1} p_{i_2} \cdots p_{i_k}$ in $Aut(L/F)$. This exhausts all subgroups of $Aut(L/F)$ and therefore produces all possible intermediate fields.

□