Algebra Exam February 2015

Show your work. Be as clear as possible. Do all problems.

1. Use Sylow's theorems and other results to describe, up to isomorphism, the possible structures of a group of order 1005.

2. Let R be a commutative ring with 1. Let M, N and V be R-modules.

   (a) Show if that M and N are projective, then so is $M \otimes_R N$.

   (b) Let $\mathrm{Tr}(V) := \{\sum_i \phi_i(v_i) | \phi \in \mathrm{Hom}_R(V, R), v_i \in V\} \subset R$. If $1 \in \mathrm{Tr}(V)$, show that up to isomorphism R is a direct summand of V^k for some k.

3. Let F be a field and M a maximal ideal of $F[x_1, \ldots, x_n]$. Let K be an algebraic closure of F. Show that M is contained in at least 1 and in only finitely many maximal ideals of $K[x_1, \ldots, x_n]$.

4. Let F be a finite field.

   (a) Show that there are irreducible polynomials over F of every positive degree.

   (b) Show that $x^4 + 1$ is irreducible over $\mathbb{Q}[x]$ but is reducible over $\mathbb{F}_p[x]$ for every prime p (hint: show there is a root in $\mathbb{F}_{p^2}$).

5. Let F be a field and M a finitely generated $F[x]$-module. Show that M is artiniian if and only if $\dim_F M$ is finite.

6. Let R be a right Artinian ring with with a faithful irreducible right R-module. If $x, y \in R$, set $[x, y] := xy - yx$. Show that if $[[x, y], z] = 0$ for all $x, y, z \in R$, then R has no nilpotent elements.

Algebra Spring 2015

① Classify groups of order 1005.

<u>solution</u> $1005 = 3\cdot 5\cdot 67.$

$n_3 = 1, \cancel{5}, 67, \cancel{5\cdot 67}$ 3-Sylow s.g. $P = \langle x\rangle$

$n_5 = 1, \cancel{3}, \cancel{67}, 3\cdot 67$ 5-Sylow s.g. $Q = \langle y\rangle$

$n_{67} = 1, \cancel{3}, \cancel{5}, \cancel{15}$ 67-Sylow s.g. $R = \langle z\rangle$

$R \trianglelefteq G$

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

In QR, $n_5 = 1, \cancel{67} \Rightarrow Q \trianglelefteq QR \overset{R \trianglelefteq QR}{\Longrightarrow} QR \cong Q\times R.$

$G \cong QR \rtimes_{\varphi} P$ determined by group maps $\varphi: P \to \mathrm{Aut}(Q\times R)$

Equiv, $\varphi : \underbrace{\langle x\rangle}_{\cong C_3} \longrightarrow \mathrm{Aut}(C_5\times C_{67}) \underset{\gcd(5,67)=1}{\cong} C_4\times C_{66} = \langle (\alpha,1),(1,\beta)\rangle$

$|\varphi(x)|\,\big|\,3 \Longrightarrow |\varphi(x)| = 1$ or 3.

So the possible φ are determined by $x \mapsto (1,\beta^{22}), (1,\beta^{44}), (1,1)$.

It is a theorem that since $\langle(1,\beta^{22})\rangle = \langle(1,\beta^{44})\rangle$ then the induced semidirect products are the same. Therefore there are only 2 isomorphism classes.

β can be taken to be

$$\beta : z \mapsto z^{l} \quad \text{for some } 2 \le l < 66.$$

Then $G \cong \langle x, y, z \mid x^3 = y^5 = z^{67} = 1, yz = zy, xy = yx, xz = z^l x \rangle$

$$G \cong C_3 \times C_5 \times C_{67}. \qquad \square$$

---

(2) R comm w/ 1. M, N, V R-modules.

(a) show if M and N are proj, then $M \otimes_R N$ is proj.

<u>solution to (a)</u>

We need to show

$$\begin{tikzcd} & M \otimes_R N \arrow[dl, dashed, "\exists \varphi"'] \arrow[d, "f"] & \\ A \arrow[r, "g"'] & B \arrow[r] & 0 \end{tikzcd}$$

Define $f_1 : M \to B$ by $f_1(m) = f(m \otimes 1)$ and $f_2 : N \to B$ by $f_2(n) = f(1 \otimes n)$; f_1 & f_2 are clearly R-mod maps. So we get maps $\varphi_1 : M \to A$ s.t. $g \circ \varphi_1 = f_1$ and $\varphi_2 : N \to A$ s.t. $g \circ \varphi_2 = f_2$. Define a map $M \times N \xrightarrow{\varphi'} A$ by $(m, n) \overset{\varphi'}{\mapsto} \varphi_1(m) + \varphi_2(n)$. By the UMP of the tensor product this induces a map

solution to (a)

Two solutions:

1) P proj $\iff \mathrm{Hom}(P, -)$ is exact.

$$\mathrm{Hom}_R(M \otimes N, -) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, -)).$$

Since M and N are exact,
$\mathrm{Hom}_R(M \otimes N, -)$ is the composition of two exact functors, hence is exact. $\square$.

2) P proj $\iff$ P is a direct summand of a free R-module.

$$M \otimes L_1 \cong R^{\oplus I_1}, \quad L_2 \otimes N \cong R^{\oplus I_2}.$$

$$(M \otimes N) \oplus \big((L_1 \oplus N) \oplus (M \oplus L_2) \oplus (L_1 \oplus L_2)\big)$$

$$\cong \big(M \otimes (N \oplus L_2)\big) \oplus \big(L_1 \otimes (N \oplus L_2)\big)$$

$$\cong (M \otimes R^{\oplus I_2}) \oplus (L_1 \otimes R^{\oplus I_2})$$

$$\cong \big((M \oplus L_1) \otimes R^{\oplus I_2}\big) \cong R^{\oplus I_1} \otimes R^{\oplus I_2}$$

$$\cong R^{\oplus (I_1 \amalg I_2)}. \ \square.$$

(b) Let $Tr(V) := \left\{ \sum_{i=1}^{n} \phi_i(v_i) : \phi_i \in \mathrm{Hom}_R(V,R), v_i \in V \right\}$ $\subset R$. If $1 \in Tr(V)$, show R is a direct summand of V^k for some k.

---

solution to (b)

Let $1 = \sum_{i=1}^{k} \phi_i(\tilde{v}_i)$.

So the R-map $V^k \xrightarrow{\varphi} R$ defined by $(v_1, \dots, v_k) \overset{\varphi}{\longmapsto} \sum_{i=1}^{k} \phi_i(v_k)$ is surj.

So we get a SES of R-modules

$$0 \longrightarrow \ker\varphi \longrightarrow V^k \xrightarrow{\varphi} R \longrightarrow 0.$$

It follows since R is a free R-module that

$$V^k \cong R \oplus \ker\varphi. \qquad \square$$

---

(3) Let k field, m maximal ideal of $k[X_1, \dots, X_n]$. Show that m is contained in at least one and in only finitely many maximal ideals of $\bar{k}[X_1, \dots, X_n]$.

<u>Solution</u> (See the end of the exam for a 'better', 'less arbitrary' solution.)

For clarity, 'maximal ideal' excludes the whole ring.

m is contained in the push-forward ideal $\bar{k}[X_1,\dots,X_n]m$ in $\bar{k}[X_1,\dots,X_n]$, which is nonunital and is thus contained in a maximal ideal M of $\bar{k}[X_1,\dots,X_n]$.

Let $E \equiv k[X_1,\dots,X_n]/m$. By Nullstellensatz, $E|k$ is a finite ext. Let $\bar{k}[X_1,\dots,X_n]$. we show there is a bijection between the set of maximal ideals M in $\bar{k}[X_1,\dots,X_n]$ containing m and the set of embeddings $E \subset \bar{k}$ extending $k \subset \bar{k}$.

Given an embedding $E \xrightarrow{\phi} \bar{k}$, i.e. $k[X_1,\dots,X_n]/m \xrightarrow{\phi} \bar{k}$, define $f(X_i) = \phi([X_i])$. This induces a surjection $\bar{k}[X_1,\dots,X_n] \xrightarrow{f} \bar{k}$ whose kernel is a maximal ideal of $\overline{K}[X_1,\dots,X_n]$ containing m, call it $F(E \xrightarrow{\phi} \overline{K})$.

Conversely, if M is a maximal ideal in $\overline{K}[X_1,\dots,X_n]$ containing m, then we have an induced embedding

$$\begin{array}{ccc} K[X_1,\dots,X_n]/m & \longrightarrow & \overline{K}[X_1,\dots,X_n]/M, \\ \| & & \cong \\ E & \overset{G(M)}{\dashrightarrow} & \overline{K} \end{array}$$

where the isomorphism $\overline{K}[X_1,\dots,X_n]/M \cong \overline{K}$ is natural given as evaluation at $(a_1,\dots,a_n)$ where $M = (X_1-a_1,\dots,X_n-a_n)$. Call the embedding $G(M)$.

It is easy to believe (see next page) F and G are inverses. Therefore, the number of maximal ideals M in $\overline{K}[X_1,\dots,X_n]$ containing m is equal to the separability degree $[E:K]_s \leq [E:K] < \infty$.

Proof that F and G are inverses. First we show $F \circ G(M) = M$. Let $M = (X_1 - a_1, \dots, X_n - a_n)$.

Then $G(M)$ is the embedding $E \xrightarrow{\phi} \bar{k}$ given by $\phi([p(X_1, \dots, X_n)]) = p(a_1, \dots, a_n)$. To determine $F(E \xrightarrow{\phi} \bar{k})$, we said consider the map $f: \bar{k}[X_1, \dots, X_n] \to \bar{k}$ given by the formula $f(p(X_1, \dots, X_n)) = p(\phi([X_1]), \dots, \phi([X_n])) =$

$= p(a_1, \dots, a_n)$. And $\ker f = \{p \in \bar{k}[X_1, \dots, X_n] \mid p(a_1, \dots, a_n) = 0\}$

$\overset{Null}{=} (X_1 - a_1, \dots, X_n - a_n) = M$. $\checkmark$

Second we show $G \circ F(E \xrightarrow{\phi} \bar{k}) = (E \xrightarrow{\phi} \bar{k})$. Where is $[p] \in E$ taken? By definition of G $[p] \in E$ is taken to $p(a_1, \dots, a_n)$ where $F(E \xrightarrow{\phi} \bar{k}) = M = (X_1 - a_1, \dots, X_n - a_n)$. How are the a_i determined? $F(E \xrightarrow{\phi} \bar{k})$ is by def the kernel of the map $\bar{k}[X_1, \dots, X_n] \xrightarrow{f} \bar{k}$ defined by $p \overset{f}{\mapsto} p(\phi([X_1]), \dots, \phi([X_n]))$. So $F(E \xrightarrow{\phi} \bar{k}) =$

$\{p \in \bar{k}[X_1, \dots, X_n] \mid p(\phi([X_1]), \dots, \phi([X_n])) = 0\} \overset{Null}{=} (X_1 - \phi([X_1]), \dots, X_n - \phi([X_n]))$.

So $F(E \xrightarrow{\phi} \bar{k}) = (X_1 - a_1, \dots, X_n - a_n)$ where $a_i = \phi([X_i])$. So referring back above, $G \circ F$ sends $[p] \in E$ to $p(a_1, \dots, a_n) = p(\phi([X_1]), \dots, \phi([X_n]))$
$= \phi([p(X_1, \dots, X_n)]) = \phi([p])$ as desired. ✓.

Notice the Nullstellensatz was crucial for both directions of the argument.

This completes the solution. $\square$.

---

(4) F_{p^n} finite field.

(a) Show there are irreducible polys over F_{p^n} of every positive degree.

(b) Show $X^4 + 1$ is irreducible over $\mathbb{Q}$ but is reducible over F_p for every prime p.

---

solution to (a)

For every n, there exists a (unique) finite field of order F_{q^n} which contains F_q as a subfield. This is a theorem. Hence $[F_{q^n} : F_q] = n$.
Moreover, F_{q^n}/F_q is simple(*)
Hence the minimal poly of the extension is the desired irreducible poly of deg n.

(*) To see F_{q^n}/F_q is simple, recall that $(F_{q^n})^\times$ is cyclic, generated by α. This says $F_{q^n} = F_q(\alpha)$. $\square$.

solution to (b)

$$(X+1)^4 + 1 = X^4 + 4X^3 + 6X^2 + 4X + \underbrace{1+1}_{=2}.$$

By Eisenstein this is irred $/ \mathbb{Q}$. ✓

If $p = 2$, then over F_2, $X^4+1 = (X+1)^4$. ✓

Let p be odd.

claim: X^4+1 divides $X^{p^2}-X$.

$p = 2n+1$. $p^2 = 4n^2+4n+1 \overset{?}{\equiv} 1 \pmod 8$.

$\iff 4(n^2+n) \overset{?}{\equiv} 0 \pmod 8$. True: n even $\Rightarrow$

n^2+n is even; n odd $\Rightarrow n^2$ odd $\Rightarrow n^2+n$ odd.

$\therefore$ $p^2 \equiv 1 \pmod 8$ So $8 \mid p^2-1$.

subclaim: X^8-1 divides $X^{p^2-1}-1$.

Use lemma: $X^a-1 \mid X^b-1$ iff $a \mid b$. ✓
(use $\Longleftarrow$ which isn't bad to check)

Hence $\underbrace{X^4+1 \mid X^8-1}_{X^4-1} \mid X^{p^2-1}-1 \mid X^{p^2}-X$. ✓

So X^4+1 splits completely in the splitting field of $X^{p^2}-X$, which is $\mathbb{F}_{p^2}$.
Let α be a root of X^4+1 in $\mathbb{F}_{p^2}$.
So $\mathbb{F}_p \subset \mathbb{F}_p(\alpha) \subset \mathbb{F}_{p^2}$. $\therefore$ Either $\mathbb{F}_p(\alpha) \cong \mathbb{F}_p$ or $\cong \mathbb{F}_{p^2}$.
If $\mathbb{F}_p(\alpha) \cong \mathbb{F}_p$, then $\alpha \in \mathbb{F}_p$ and $X-\alpha \mid X^4+1$ in $\mathbb{F}_p[X]$. If $\mathbb{F}_p(\alpha) \cong \mathbb{F}_{p^2}$, then $[\mathbb{F}_p(\alpha):\mathbb{F}_p]=2$.
So the minimal poly $m_\alpha(X)$ of α in $\mathbb{F}_p[X]$ has deg 2. so $m_\alpha(X) \mid X^4+1$ in $\mathbb{F}_p[X]$. $\square$

(5) F field. M f.g. F[x]-module.

Show M Artinian iff $\dim_F M < \infty$.

<u>solution</u>

$$M \cong \underbrace{F[x]^r}_{\substack{\text{Artinian} \\ \text{iff } r=0 \\ \text{\& infinite} \\ \dim /F.}} \oplus \underbrace{\frac{F[x]}{(d_1(x))} \oplus \cdots \oplus \frac{F[x]}{(d_n(x))}}_{\text{f.d. }/F \text{ so Artinian}}.$$

$\square$

(6) R right Artinian w/ a faithful irreducible (i.e. simple) right R-module. Show if $[[x, y], z] = 0$ for all $x, y, z \in R$, where $[x, y] = xy - yx$, then R has no nilpotent elements.

Solution

The Jacobson radical J of R is

$$J = \bigcap_{\substack{N \text{ nonzero} \\ \text{simple right} \\ R\text{-module}}} \Big\{ \underbrace{a \in R : na = 0 \ \forall n \in N}_{\mathrm{Ann}(N_R)} \Big\}.$$

By definition, a right R-module N_R is faithful if $\mathrm{Ann}(N_R) = 0$.

So $J = 0$. Since in addition R is right Artinian, R is semisimple. By Artin-Wedderburn,

$$R \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$$

If $n_i = 1$ for all i, then R has no nilpotents.

It suffices to show over any ring S that $M_2(S)$ does not satisfy $[[x,y],z]=0 \ \forall x,y,z$.

Let $\{e_{ij}\}$ be the standard basis for $M_N(S)$. Then $[e_{ij}, e_{kl}] = \delta_{jk} e_{il} - \delta_{li} e_{kj}$.

So $[[e_{ij}, e_{kl}], e_{mn}] = \delta_{jk}[e_{il}, e_{mn}] - \delta_{li}[e_{kj}, e_{mn}] =$

$= \delta_{jk}\delta_{lm}e_{in} - \delta_{jk}\delta_{ni}e_{ml} - \delta_{li}\delta_{jm}e_{kn} +$

$+ \delta_{li}\delta_{nk}e_{mj}$. Taking $\boxed{j=k,\ l=m}$ this

equals $e_{in} - \delta_{ni}e_{ll} - \delta_{li}\delta_{jl}e_{jn} +$

$+ \delta_{li}\delta_{nj}e_{lj}$. Taking $\boxed{l \neq i,\ n \neq i}$ this

equals just e_{in}. we can solve for these

conditions in $M_2(S)$: $i=1,\ j=k=l=m=n=2$.

So we have a contradiction. check:

$$[e_{12}, e_{22}] = \begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix} - \begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix} = \begin{pmatrix}0&1\\0&0\end{pmatrix} - \begin{pmatrix}0&0\\0&0\end{pmatrix}.$$

$$[[e_{12}, e_{22}], e_{22}] = \begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix} - \begin{pmatrix}0&0\\0&1\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix} = \begin{pmatrix}0&1\\0&0\end{pmatrix} - \begin{pmatrix}0&0\\0&0\end{pmatrix}.$$

This proves $R \cong D_1 \times \cdots \times D_K$ and hence

has no nilpotents. $\square$

Alternate solution to Problem 3

Lemma/ If $f(X_i) \in (X_1 - a_1', \ldots, X_n - a_n') \cap \bar{k}[X_1, \ldots, X_n]$ then a_i' is a root of $f(X_i)$.

Proof/ This is an immediate consequence of the Nullstellensatz. Indeed, $(X_1 - a_1', \ldots, X_n - a_n')$ equals $I(a_1', \ldots, a_n') = \{f \in \bar{k}[X_1, \ldots, X_n] : f(a_1', \ldots, a_n') = 0\}$.

So $f(X_i)$ evaluated at $(a_1, \ldots, a_n)$ equals 0, i.e. $f(a_i') = 0$. ✓.

Let M be a maximal ideal of $\bar{k}[X_1, \ldots, X_n]$ containing m. Then $m \subset M \cap k[X_1, \ldots, X_n]$ and this intersection is an ideal of $k[X_1, \ldots, X_n]$, so $m = M \cap k[X_1, \ldots, X_n]$ by maximality. Let $M = (X_1 - a_1, \ldots, X_n - a_n)$ by Null. So $m = M \cap k[X_1, \ldots, X_n]$ contains the minimal polys $m_i(X_i)$ of the a_i. Suppose M' is another such maximal ideal of $\bar{k}[X_1, \ldots, X_n]$ containing m. So $M' = (X_1 - a_1', \ldots, X_n - a_n')$. Since the previous minimal polys $m_i(X_i)$ are in $m \subset M'$, we claim $X_i - a_i' \mid m_i(X_i)$, i.e. a_i' is a root of $m_i(X_i)$. Indeed, $m_i(X_i) \in M' = \{f \in \bar{k}[X_1, \ldots, X_n] : f(a_1', \ldots, a_n') = 0\}$. (This is the lemma above.) Since $m_i(X_i)$ has only finitely many roots, there are only finitely many choices for a_i'. $\square$