ALGEBRA PH.D QUALIFYING EXAM SPRING 2007

done

1. For G a finite group with $|G| > 1$ and p a prime dividing the order of G, let $O_p(G) = \bigcap\{P \in Syl_p(G)\}$.
   a) Show that $O_p(G)$ is a normal subgroup of G.
   b) Show that if N is a normal subgroup of G with $|N| = p^k$, then $N \subseteq O_p(G)$.
   c) Prove that if G is solvable then for some p, $|O_p(G)| \neq 1$.

$N \triangleleft G$. $p \,/\, |N|$

2. Let $F = GF(p^n)$ be a field of (exactly) p^n elements. Suppose that k is a positive integer dividing n, and set $B = \{ a^{p^k} + a^{p^{2k}} + \cdots + a^{p^n} \mid a \in F\}$.
   i) Show that $B \subseteq E$, a subfield of F with p^k elements.
   ii) Show that $B = E$.

3. Let $A \in M_n(Q)$ with $A^k = I_n$. If j is a positive integer with $(j, k) = 1$, show that $\mathrm{tr}(A) = \mathrm{tr}(A^j)$. (Hint: Consider $A \in M_n(Q(\varepsilon))$ for $\varepsilon = e^{2\pi i/k}$, where $i^2 = -1$.)

4. Let R be a commutative ring with 1 and let M be a Noetherian R-module. If $f \in \mathrm{Hom}_R(M_R, M_R)$ is surjective, show that f is an automorphism of M_R.

5. Let $f, g \in \mathbf{C}[x, y]$ so that $(0, 0) \in \mathbf{C}^2$ is the only common zero of f and g. Prove that there is a positive integer m so that whenever $h \in \mathbf{C}[x, y]$ has no monomial of degree less than m, then $h \in f\cdot\mathbf{C}[x, y] + g\cdot\mathbf{C}[x, y]$.

6. For a fixed positive integer $n > 1$, describe all finite rings R so that $x^n = x$ for all $x \in R$.

E/B

Algebra: Spring 2007:

① $|G| < \infty$, $p \mid |G|$, let $O_p(G) = \bigcap_{P \in Syl_p(G)} P$

(a) Show that $O_p(G)$ is normal s.g. of G

For $g \in G$, define $\varphi_g : G \to G$ as conjugation by g. Note that $O_p(G)$ is contained in every Sylow p-s.g., hence $O_p(G) \subseteq P \ \forall P$ implies $\varphi_g(O_p(G)) \subseteq \varphi_g(P)$ for all P.

Recall by Sylow that all Sylow s.g.'s are conjugate to each other, hence as P ranges over all $Syl_p(G)$, so does $\varphi_g(P)$, hence $\varphi_g(O_p(G))$ is in all Sylow p-subgroups, i.e. $\varphi_g(O_p(G)) \subseteq O_p(G)$, Hence $O_p(G) \trianglelefteq G$.

(b) If $N \trianglelefteq G$ with $|N| = p^k$, then $N \subseteq O_p(G)$

If $N \trianglelefteq G$, then $gNg^{-1} = N \ \forall g \in G$

$|N| = p^k \Rightarrow N \leq S$ for some Sylow p-subgroup of G

$\Rightarrow gNg^{-1} \leq gSg^{-1} = S'$, another Sylow p-subgroup.

So $N = gNg^{-1} \leq S_1$, hence $N \leq S_1$ as well; now ranging over all $g \in G$, we get that N is contained in every Sylow p-s.g., hence $N \leq O_p(G)$.

(c) If G solvable, then $|O_p(G)| \neq 1$ for some p

If G is solvable, then there is minimal normal s.g. $N \trianglelefteq G$ with $N = (\mathbb{Z}_p)^k$. Hence $|N| = p^k$, hence $N \subseteq O_p(G)$ by (b), hence $|O_p(G)| \neq 1$ (Proof of underline: Cf. #2 FEB'02; consider the commutator, $[N,N]$; show $[N,N] \trianglelefteq G$; show $N \supsetneq \{e\}$ by minimality of N; then N finite-abelian & get order by minimality arguments again)

② $F=\mathbb{F}_{p^n}$, $k|n$, $B=\{a^{p^k}+a^{p^{2k}}+\cdots+a^{p^n} : a\in F\}$

(i) Show $B\subseteq E$, $E=\mathbb{F}_{p^k}\subseteq F$:

see that for $(a^{p^k}+a^{p^{2k}}+\cdots+a^{p^n})\in B$ we have:
$(a^{p^k}+a^{p^{2k}}+\cdots+a^{p^n}) = (a^{p^k}+a^{p^{2k}}+\cdots+a^{p^{n-k}}+a)$
$= (a+a^{p^k}+\cdots+a^{p^{n-k}})$

Now see that, since $a^{p^n}=a$ and characteristic p in F:

$(a+a^{p^k}+\cdots+a^{p^{n-k}})^{p^k} = (a^{p^k}+a^{p^{2k}}+\cdots+a^{p^n})$
$= (a+a^{p^k}+\cdots+a^{p^{n-k}})$

So all elts in B satisfy $x^{p^k}-x$, hence all are in $\mathbb{F}_{p^k}$.

(ii) Show $B=E$:

For $b\in B$ we showed $b^{p^k}=b$, hence each element has an inverse.
Also, since char. p, $(a^{p^k}+\cdots+a^{p^n})+(b^{p^k}+\cdots+b^{p^n}) = (a^{p^k}+b^{p^k})+\cdots+(a^{p^n}+b^{p^n})$
$= (a+b)^{p^k}+\cdots+(a+b)^{p^n} \in B$

Therefore B is a field, ~~and thus~~

Now consider the extension F/E, i.e. $\mathbb{F}_{p^n}/\mathbb{F}_{p^k}$.
We know $\frac{n}{k}=[F:E]=|\mathrm{Gal}(F/E)|$, ~~hence~~:
$\mathrm{Gal}(F/E)=\langle\sigma:\alpha\mapsto\alpha^{p^k}\rangle$

Now consider the trace map $T_{F/E}: F\to E$
$\alpha\mapsto\sum_{\sigma\in\mathrm{Gal}(F/E)}\sigma(\alpha)$
$=\alpha^{p^k}+\alpha^{p^{2k}}+\cdots+\alpha^{p^n}\in B$

Hence $\mathrm{Tr}(F)=B$

Now, Tr is a linear map from an $\frac{n}{k}$-dim'l E-v.s. to a 1-dim'l E-v.s., hence if $\mathrm{Tr}\neq 0$ it is surjective; By linear independence of characters, which members of $\mathrm{Gal}(F/E)$ are, Tr is not identically zero, hence $E=\mathrm{Tr}(F)=B$.

③ $A \in M_n(\mathbb{Q})$, $A^k = I_n$. If j positive with $\gcd(j,k)=1$, show that $tr(A) = tr(A^j)$.

$A^k = I_n \Rightarrow A$ invertible $\Rightarrow A$ has no zero eigenvalue.

Now, $\lambda^k v = A^k v = Iv = v$, hence roots of $x^k - 1$ are the distinct eigenvalues of A, (with possible

Let ω be a primitive k^{th} root of unity and consider the extension $\mathbb{Q}(\omega)/\mathbb{Q}$ with $Gal(L/\mathbb{Q}) \cong \mathbb{Z}_k^{\times} \cong \langle \varphi : \omega \mapsto \omega^j, \rangle$
$\gcd(j,k)$

Now, see that $Tr(A) = \sum_{i=1}^{n} \lambda_i$ and let $\gcd(j,k)=1$:

Then see that $Tr(A^j) = \sum_{i=1}^{n} \lambda_i^j = \sum_{i=1}^{n} \varphi(\lambda_i) = \sum_{i=1}^{n} \lambda_i = Tr(A)$

(Since φ is an bijection of $\{\lambda_i\}$)

④ R commutative ring with 1 and let M be a noeth R-module. If $f \in Hom_R(M_R, M_R)$ surj, show it is an automorphism

---

$\varphi : M \to M$ surjective on R-modules.

Since M noeth, the chain $\ker\varphi \subseteq \ker\varphi^2 \subseteq \cdots \subseteq \ker\varphi^n = \ker\varphi^{n+1}$ terminates at some n.

Since φ surjective, φ^k surjective for all k.

Choose $x \in \ker\varphi$; then $\exists y \in M$ s.t. $\varphi^n(y) = x \Rightarrow \varphi^{n+1}(y) = \varphi(x) = 0$

$\Rightarrow y \in \ker\varphi^{n+1} = \ker\varphi^n$

$\Rightarrow 0 = \varphi^n(y) = x$

So $\ker\varphi = 0$, hence inj + surj $\Rightarrow x = 0$

$\underline{= \text{autom}}$.

(5) $f, g \in \mathbb{C}[x,y]$ s.t. $(0,0) \in \mathbb{C}^2$ is the only common zero of f & g. Prove $\exists\, m > 0$ s.t. if $h \in \mathbb{C}[x,y]$ has no monomial of degree $\leq m$, then $h \in (f)+(g)$.

Recall $Var((f)+(g)) = Var(f) \cap Var(g) = \{(0,0)\}$
and thus $\sqrt{(f)+(g)} = Id(Var((f)+(g))) = Id(\{(0,0)\}) = (x,y)$.
Hence $\exists\, m$ such that $x^m, y^m \in (f)+(g)$.
Hence if $h \in \mathbb{C}[x,y]$ and every monomial has total degree $\geq 2m$, then every monomial is in $(f)+(g)$, hence $h \in (f)+(g)$.

---

(6) For $n > 1$, describe all finite rings s.t. $x^n = x$ $\forall x \in R$.

R finite $\Rightarrow$ R artinian $\Rightarrow$ $J(R)$ nilpotent
But $x^n = x$ $\forall x$ $\Rightarrow$ no nilpotent elements. $\Rightarrow J(R) = 0$.
Therefore artinian & J.S.S $\Rightarrow$ S.S.
$\Rightarrow R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$, but R finite, so D_i's finite.
so $D_i = F_i$ fields by little wedd.; no nilp elts, so $n_i = 1$ $\forall i$.
$\Rightarrow R \cong F_1 \oplus \cdots \oplus F_k$; $x \in R$ has $x = (a_1, \ldots, a_k)$
$x = x^n$ $\forall x \in R \Rightarrow a_i^n = a_i$ $\forall a_i \in F_i$. Therefore $|F_i| \leq n$ for all i,
Each $|F_i^\times| = p_i^{e_i} - 1$, so $p_i^{e_i} - 1 \mid n-1$ for all i.