ALGEBRA QUALIFYING EXAM, Spring 2009

Throughout, $\mathbb{Z}$ denotes the integers, $\mathbb{Q}$ the rational numbers, $\mathbb{R}$ the real numbers, and $\mathbb{C}$ the complex numbers.

1. Let G be a finite group. Define the *Frattini subgroup* of G to be $\Phi(G)$, the intersection of all maximal subgroups of G.
   (1) Show that $\Phi(G)$ is characteristic in G (i.e. invariant under any automorphism of G).
   (2) Show that if $G = \langle \phi(G), S \rangle$ for some subset S of G, then $G = \langle S \rangle$.
   (3) Let P be a Sylow p-subgroup of $\phi(G)$. Show that P is normal in G (hint: first show that $G = \Phi(G)N_G(P)$ by using Sylow's theorems and then use (2)).
   (4) Show that $\Phi(G)$ is nilpotent.

2. Let G be a finite group acting on the finite set X with $|X| = n > 1$, and suppose that G has N orbits on X. If $g \in G$, let $F(g)$ be the number of $x \in X$ fixed by g.
   (1) Prove that $\sum_{g \in G} F(g) = |G|N$ (this is known as *Burnside's Lemma*).
   (2) Prove that if G is transitive on X, then $F(g) = 0$ for some $g \in G$ (either use (1) or prove directly).
   (3) Show that this is not always true if G is not transitive on X.

3. Let $f(x) = x^4 - x^3 + x^2 - x + 1 \in \mathbb{Q}[x]$. Find the splitting field (over $\mathbb{Q}$) of $f(x)$, and compute $Gal(K/\mathbb{Q})$.

4. Construct an example of each of the following (with reasons):
   (1) A field extension $F \subsetneq K$ which is normal but not separable.
   (2) A field extension $F \subsetneq K$ which is separable but not normal.
   (3) A field extension $F \subsetneq K$ which is neither separable nor normal.

5. Let F be the field of p elements. Let $A \in G := GL(n, F)$.
   (1) Show that A has order a power of p if and only if $(A - I)^n = 0$.
   (2) Show that if this is the case then the order of A is less than np.
   (3) Show that any such A is similar to an upper triangular matrix.

6. Let M be a finitely generated abelian group, and N a subgroup. If $M \otimes_{\mathbb{Z}} \mathbb{Q} \cong N \otimes_{\mathbb{Z}} \mathbb{Q}$, show that M/N is torsion.

CONTINUED →

7. Consider the polynomial ring $\mathbb{C}[x, y]$ and let I be the ideal $I = (x + y - 2, x^2 + y^2 - 10)$.

(1) Show that there exists some $m > 0$ such that, $(3x^2 + 10xy + 3y^2)^m \in I$.

(2) Show that the two ideals $I_1 = (x + y - 2)$ and $I_2 = (x^2 + y^2 - 10)$ are prime ideals. Are they maximal?

(3) Can I be written as an intersection of maximal ideals? Why or why not?

see Fall 2006 #6

8. Let A be a finite-dimensional algebra over $\mathbb{R}$, with center $Z = Z(A)$ and Jacobson radical $J = J(A)$. Assume that for any $a \in A$, there is some $n = n(a) \geq 1$ such that $a^{2^n} - a \in Z$.

(1) Show that $J \subseteq Z$.

(2) Show that A/J is commutative.

In fact A itself is commutative, although you do not have to show this.

$x+y-2$

$I_1 \subseteq I$
$I_2 \subseteq I$

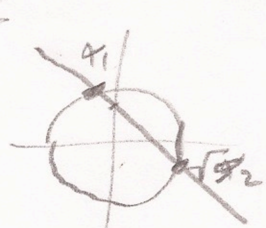
$(x+y-2)^2 = (x+y-2)(x+y-2)$
$= \cancel{x^2} + \cancel{xy} - 2x + \cancel{yx} \cancel{y^2}$
$-2y - 2x - 2y + 4$

$(x+y)(x+y) = x^2+y^2+2xy$
$\cancel{(x+y)(x+y-xy)}$

$= x^2+y^2+2xy - 4x - 4y + 4$
$\cancel{= x^2+y^2+2xy - 4(x+y-1)}$
$\cancel{\Rightarrow x^2+y^2+2xy+4}$

$x+y-2 = x^2+y^2-10$
$\Rightarrow x+y+8 = x^2+y^2$
$x - x^2 = y^2 - y - 8$

$x+y=2$
$x^2+y^2=10$



$I = I_1 + I_2$

$\Rightarrow Var(I) = Var(I_1+I_2) = Var\, I_1 \cap Var\, I_2$
$= \{\alpha_1, \alpha_2\}$

$\sqrt{I} = Id(Var(I)) = Id(Var(I_1+I_2)) \equiv Id(Var\, I_1 \cap Var\, I_2)$
$= \sqrt{(X-\alpha_1) \cap (X-\alpha_2)} = (X-\alpha_1) \cap (X-\alpha_2)$

① $|G|<\infty$, $\Phi(G)\leq G$ intersection of all maximal subgroups in G.

(a) Show that $\Phi(G)$ is invariant under any automorphism of G.

Let $\varphi: G\to G$ be an automorphism, and suppose $M \lneq G$ is maximal. Clearly $\varphi(M)$ is a subgroup; now we'll show it is maximal:

$$\text{Suppose } \varphi(M) \lneq N \lneq G \Rightarrow M \leq \varphi^{-1}(N) \Rightarrow M = \varphi^{-1}(N) \quad \text{inv. exists since Aut.}$$
$$\Rightarrow \varphi(M) \geq N$$

Hence $\varphi(M)=N$, hence $\varphi(M)$ is maximal.

- Now suppose M_1 & M_2 are distinct maximal subgroups, and note that $\varphi(M_1)\neq\varphi(M_2)$ for $M_1\neq M_2$ or else injectivity would be contradicted. Therefore φ maps maximal s.g.'s to maximal s.g.'s injectively.

- Now consider $g\in\Phi(G) \Rightarrow g\in M$ $\forall$ max'l s.g.'s M.

$\Rightarrow \varphi(g)$ in all max. s.g.'s since φ maps max sg $\leftrightarrow$ max sg injectively.

$\Rightarrow \varphi(g)\in\Phi(g)$

$\longrightarrow \underline{\Phi(g)\subseteq\varphi(\Phi(g))}$

(b) Show if $G=\langle\Phi(G),S\rangle$ for some $S\subseteq G$, then $G=\langle S\rangle$

Suppose $G=\langle\Phi(G),S\rangle$, $S\subseteq G$. Now consider $\langle S\rangle = \bigcap_{\substack{H\leq G\\ S\subseteq H}} H$

Suppose $\langle S\rangle \lneq G$; then either $\langle S\rangle$ is a maximal subgroup or it is contained in one.

- If $\langle S\rangle$ is maximal, then $\Phi(G)\leq\langle S\rangle$, i.e. $\underline{\langle S\rangle=\langle S,\Phi(G)\rangle=G}$.
- If $\langle S\rangle$ is not maximal, $\exists$ max sg. M s.t. $\langle S\rangle\leq M$; but $\Phi(G)\leq M$ as well, so $\langle S,\Phi(G)\rangle\leq M\lneq G$, contradiction.

Hence $\langle S\rangle$ must be maximal, hence $\underline{\langle S\rangle = G}$.

(c) $P \le \Phi(G)$ Sylow p-subgroup ; Show $P \trianglelefteq G$.

Step 1 : (Lemma) $H \trianglelefteq G$, $P \le H$ Sylow p-s.g. ; then $\forall g \in G$, $\exists x \in H$ w/ $gPg^{-1} = xPx^{-1}$:

Pf: Choose $g \in G$; then $gPg^{-1} \le H$ since $P \le H$ & H normal in G, but $|gPg^{-1}| = |P|$, hence gPg^{-1} also a Sylow p-sgs hence by Sylow thms, gPg^{-1} is a conjugate of P in H, i.e. $\exists x \in H$ such that $xPx^{-1} = gPg^{-1}$!

Step 2 : Now see that $\boxed{P \le \Phi(G) \trianglelefteq G}$ (normal since invariant under all automorphisms by (a)).

Choose $g \in G$; so by Step 1, $gPg^{-1} = fPf^{-1}$ for some $f \in \Phi(G)$.

Now recall that $N_G(P) = \{g : gPg^{-1} = P\}$. See that since $gPg^{-1} = fPf^{-1}$ we have $p_1, p_2 \in P$ such that $gp_1g^{-1} = fp_2f^{-1} \Rightarrow g = \underbrace{fp_2}_{\Phi(G)}\underbrace{f^{-1}gp_1}_{N_G(P)}$

, $f \in \Phi(G)$, $p_2 \in P$; but $P \le \Phi(G)$, hence $fp_2 \in \Phi(G)$

$\cdot\ f^{-1}gp_1^{-1}Pp_1g^{-1}f = f^{-1}gPg^{-1}f = f^{-1}fPf^{-1}f = P$

$p_1 \in P$ hence $f^{-1}gp_1 \in N_G(P)$

Therefore $G = \Phi(G)N_G(P)$

Step 3 : So now $G = \langle \Phi(G), N_G(P) \rangle \underset{\text{By part (b).}}{=} \langle N_G(P) \rangle \Rightarrow N_G(P) = G$

$\Rightarrow P \trianglelefteq G$.

(d) Show that $\Phi(G)$ nilpotent :

Let $P \le \Phi(G)$ be a Sylow p-s.g. Then $P \trianglelefteq G$ by (c), hence $P \trianglelefteq \Phi(G)$, hence P is unique. True for all Sylow p-s.g's of $\Phi(G)$, hence $\Phi(G)$ is a direct sum of its Sylow p-subgroups $\Leftrightarrow$ nilpotent.

(2) $|G|, |X| = n < \infty$, $G \circlearrowright X$, and suppose G has N orbits on X.
If $g \in G$, let $F(g) = \#\{x \in X : gx = x\}$.

(a) Prove $\sum_{g \in G} F(g) = |G| \cdot N$ (Burnside's Lemma)

cf. Rotman p. 76.

(b) If $G \circlearrowright X$ transitive, then $F(g) = 0$ for some $g \in G$.

Transitive $\Rightarrow$ # orbits $= N = 1$

Suppose $F(g) \geq 0$ $\forall g \in G$. Then since $\sum_{g \in G} F(g) = |G|$ (By pf. (a)), we have that $F(g) \leq 1$, i.e. $F(g) = 1$; but $F(e) = |X|$, so contradiction; hence there must be $F(g) = 0$ for some $g \in G$.

③ $f(x) = x^4 - x^3 + x^2 - x + 1 \in \mathbb{Q}[x]$. Find the splitting field & galois group. 3.

Recall that $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$ ← irreducible over $\mathbb{Q}$.

See that $(-x)^5 - 1 = (-x-1)(x^4 - x^3 + x^2 - x + 1)$, ← still irreducible.

hence if $w^5 = 1$, then $-w$ is a root of $x^4 - x^3 + x^2 - x + 1$

Therefore $\mathbb{Q}(\omega)/\mathbb{Q}$ is a splitting field (Galois ext. since cyclotomic).

Now, we know $Gal(\mathbb{Q}(\omega)/\mathbb{Q}) = Units(\mathbb{Z}_5) = \mathbb{Z}_5^* \cong \mathbb{Z}_4$

④ Construct example of each:

(a) K/F separable, but not normal:

Consider the polynomial $x^5 + 2$; let $w^5 = 1$, and then the roots are $-w^j \sqrt[5]{2}$. Therefore $\mathbb{Q}(\sqrt[5]{2})/\mathbb{Q}$ is a separable extension since characteristic zero, but not normal since x^5+2 has a root in $\mathbb{Q}(\sqrt[5]{2})$ but does not factor into linear factors in $\mathbb{Q}(\sqrt[5]{2})$ since $w \notin \mathbb{Q}(\sqrt[5]{2})$.

(b) K/F normal, but not separable:

Consider $\mathbb{F}_p(t)(\alpha)$ | $\mathbb{F}_p(t)$ ← transcendental elt.

where $x^p - t \in \mathbb{F}_p(t)[x]$

let $\alpha^p = t$; then $(x-\alpha)^p$ is the factorization in $\mathbb{F}_p(t)(\alpha)$, hence extension normal, but not separable

(c) K/F neither

$q > 3$

$\mathbb{F}_q(t)(\alpha)$ | $\mathbb{F}_q(t)$

where $x^3 - t \in \mathbb{F}_p(t)$; let $\alpha^3 = t$ & $w^3 = 1$

but the roots of $x^3 - t$ are $\alpha, w\alpha, w^2\alpha$

⑤ F field of p elements. Let $A \in G := GL_n(F)$.

(a) Show $\operatorname{ord}(A)$ power of $p \iff (A-I)^n = 0$

($\Rightarrow$) Suppose $A^{p^k} = I$; then $0 = A^{p^k} - I = (A-I)^{p^k}$ since $\operatorname{char}(F) = p$.
So $(A-I)^{p^k} = 0$, i.e. $f(x) = x^{p^k}$ has $A-I$ as a root, hence for m the minimal poly of $A-I$, $m(x) \mid x^{p^k}$, hence $m(x) = x^l$;
but $\deg m(x) \leq n$, hence $(A-I)^n = 0$.

($\Leftarrow$) Suppose $(A-I)^n = 0$. Then $\exists\, k$ such that $p^k > n$, so $(A-I)^{p^k} = 0$
$\Rightarrow A^{p^k} - I = 0 \Rightarrow A^{p^k} = I$; but $\operatorname{ord}(A) \mid p^k \Rightarrow \operatorname{ord}(A) = p^m$ $(m \leq k)$

(b) Show if this is the case, then the $\operatorname{ord}(A) < np$.

Suppose $(A-I)^n = 0 \Rightarrow (A-I)^{np} = 0 \Rightarrow A^{np} - I = 0 \Rightarrow A^{np} = I$
Hence $\operatorname{ord}(A) \mid np$. By (a), $\operatorname{ord}(A)$ a power of p.

- If $n = p^k$: we have $(A-I)^{p^k} = A^{p^k} - I \Rightarrow A^{p^k} = I \Rightarrow \operatorname{ord}(A) \mid p^k$,
hence $\operatorname{ord}(A) \leq n = p^k < p^{2k} = pn$

- If $n = p^k m$, $p \nmid m$: $\operatorname{ord}(A)$ a power of p & $\operatorname{ord}(A) \mid p^{k+1} m$
Then $\operatorname{ord}(A) \leq p^{k+1} < p^{k+1} m$

(c) Show such an A is similar to an upper-triangular matrix

Recall $F = \mathbb{F}_p$. Now we will find $|GL_n(F)|$. There are $p^n - 1$ choices for the first column vector. Now, the second column vector can't be a multiple of the first, hence there are $p^n - p$ choices for the 2nd (since there are p multiples of the first column vector over $\mathbb{F}_p$).

Hence continue in this manner to see: $|GL_n(F)| = (p^n-1)(p^n-p)\cdots(p^n - p^{n-1})$
$= (p^n-1)\, p\, (p^{n-1}-1)\, p^2 (p^{n-2}-1) \cdots p^{n-1}(p-1) = p^{1+2+\cdots+(n-1)} k$, where $\gcd(k,p) = 1$.
$= p^{\frac{n(n-1)}{2}} k$; hence $GL_n(F)$ has a Sylow p-sg. of order $p^{\frac{n(n-1)}{2}}$. Now see that $\begin{bmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$ has this order, hence $P = \left\{ \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \right\}$ a Sylow p-sg.; A has order power p,
hence $\langle A \rangle \leq S P S^{-1}$ for some $S \in GL_n(F)$, hence A similar to upper-Δ matrix.

⑥ M finitely gen abelian group, $N \le M$. If $M \otimes_{\mathbb{Z}} \mathbb{Q} \cong N \otimes_{\mathbb{Z}} \mathbb{Q}$, show that M/N is torsion.

$M \cong \mathbb{Z}^n \oplus \mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{e_k}}$

$N \cong \mathbb{Z}^m \oplus \mathbb{Z}_{p_1^{f_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{f_k}}$

$M \otimes_{\mathbb{Z}} \mathbb{Q} \cong (\mathbb{Z}^n \oplus \mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{e_k}}) \otimes \mathbb{Q}$

$\cong (\mathbb{Z}^n \otimes \mathbb{Q}) \oplus (\mathbb{Z}_{p_1^{e_1}} \otimes \mathbb{Q}) \oplus \cdots \oplus (\mathbb{Z}_{p_k^{e_k}} \otimes \mathbb{Q})$

$(n \otimes q) = \frac{p_1^{e_1}}{p_1^{e_1}} (n \otimes q)$

$= p_1^{e_1} n \otimes \frac{q}{p_1^{e_1}}$

$= 0 \otimes \frac{q}{p_1^{e_1}} = 0 \otimes 0$

$\Rightarrow \mathbb{Z}_{p_i^{e_i}} \otimes \mathbb{Q} \cong 0 \ \forall i$

$\cong (\mathbb{Z}^n \otimes \mathbb{Q}) \oplus 0 \oplus \cdots \oplus 0 \cong \mathbb{Z}^n \otimes_{\mathbb{Z}} \mathbb{Q}$

$\cong (\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q} \cong (\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q})^n \cong \mathbb{Z}^n$

Hence we also have $N \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Z}^m$, hence $\mathbb{Z}^m \cong N \otimes \mathbb{Q} \cong M \otimes \mathbb{Q} \cong \mathbb{Z}^n$

hence $m = n$. Then: $M/N \cong \mathbb{Z}^m/\mathbb{Z}^m \oplus$ (torsion part)

$\cong 0 \oplus$ (torsion part) $\Rightarrow$ M/N torsion.

⑦ $\mathbb{C}[x,y]$, $I = (x+y-2, x^2+y^2-10) \subseteq \mathbb{C}[x,y]$

(a) Show that $\exists\, m > 0$ s.t. $(3x^2+10xy+3y^2)^m \in I$

$(3x^2+10xy+3y^2)^m \in I \iff 3x^2+10xy+3y^2 \in \sqrt{I} = Id(Var(I))$

$\iff 3x^2+10xy+3y^2$ vanishes on $Var(I)$

Let $(a,b) \in Var(I)$

Then $a+b-2=0 \Rightarrow a+b=2 \Rightarrow a^2+2ab+b^2=4 \Rightarrow 2ab+10=4 \Rightarrow 2ab=-6$

$a^2+b^2-10=0 \Rightarrow a^2+b^2=10$

$\Rightarrow ab=-3$

so $3a^2+10ab+3b^2 = 3a^2+3b^2-30$

$= 3(a^2+b^2)-30 = 30-30 = 0$

hence $3x^2+10xy+3y^2$ vanishes on $Var(I)$ $\rightsquigarrow$ $(3x^2+10xy+3y^2)^m$ for some $m>0$.

(b) The ideals $I_1 = (x+y-2)$ & $I_2 = (x^2+y^2-10)$ are prime. Maximal?

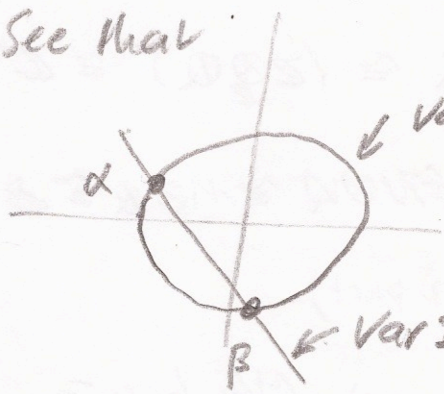
- $x+y-2$ all linear terms, so irreducible, hence I_1 prime
- Consider x^2+y^2-10 as a polynomial in $\mathbb{C}[x][y]$.

Then $x^2+y^2-10 = y^2 + (x-\sqrt{10})(x+\sqrt{10})$, hence irreducible by Eisenstein with $p = (x-\sqrt{10})$, a prime in $\mathbb{C}[x]$.

Therefore I_2 is prime.

(c) $I = I_1 + I_2$ intersection of max ideals?

See that



so $Var\, I_1 \cap Var\, I_2 = \{\alpha, \beta\}$
$\quad = Var(I_1 + I_2)$

so now $\sqrt{I} = Id(Var(I_1+I_2)) = Id(Var\{\alpha,\beta\})$
$= (x-\alpha) \cap (x-\beta)$

since $I \subseteq \sqrt{I}$, $I \subseteq (x-\alpha)$ & $I \subseteq (x-\beta)$

I cannot be contained in another max ideal, hence only the radical of I is $\cap$ of max ideals

(8) A fin-dim'l $\mathbb{R}$-algebra, $Z = Z(A)$, $J = J(A)$.
Assume for any $a \in A$, $\exists\, n = n(a) \geq 1$ s.t. $a^{2^n} - a \in Z$

(a) Show that $J \subseteq Z$:

A fin-dim'l $\mathbb{R}$-algebra so artinian, hence $J(A)^m = 0$.
Now consider $A/Z(A)$; any elt $a \in A/Z(A)$ has $a^{2^n} - a = 0 \Rightarrow a^{2^n} = a \,|= 0$
$\Rightarrow$ no nilpotent elements

Now choose $k \in J(A)$ and consider $\bar{k}$ in $A/Z(A)$; but $k^m = 0$, hence a zero divisor, hence cannot satisfy $k^{2^n} = k$, hence $k = 0$, that is, $k \in Z(A)$. $\Rightarrow$ Hence, $\underline{J(A) \subseteq Z(A)}$.

(b) A/J is commutative:

A artinian, hence so is A/J; also Jacobson s.s. $\Rightarrow$ semisimple.
By Art-Wedd ~~A/J is~~
$$A/J \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$$

(?)

$$a^{2^n} - a \in Z(A) \Rightarrow (2a)^{2^n} - 2a \in Z(A)$$
$$\Rightarrow 2^{2^n} a^{2^n} - 2a \in Z(A)$$
$$\Rightarrow 2^{2^n}(a + z) - 2a \in Z(A)$$
$$\Rightarrow (2^{2^n} - 2)a + 2^{2^n} z \in Z(A)$$
$$\Rightarrow (2^{2^n} - 2)a \in Z(A) \Rightarrow a \in Z(A)$$

Suppose a is nilpotent. Then $a^m = 0$ some minimal m.
Now, $a^{2^{n_1}} - a \in Z(A/J) \Rightarrow (a^{2^{n_1}})^{2^{n_2}} - a^{2^{n_1}} \in Z(A/J)$
$\Rightarrow a^{2^{n_1+n_2}} - a^{2^{n_1}} \in Z(A/J)$; hence we may continue until $2^{n_1+n_2+\cdots+n_\ell} > m$, and we get ~~$+$~~ $a^{2^{n_1+\cdots+n_{\ell-1}}} \in Z(A/J) \Rightarrow a \in Z(A/J)$ by backtracking.

Therefore every nilpotent elt. is in the center, but $A/J(A)$ has no central nilpotent elements, hence $A/J(A)$ has no nilpotent elts, hence $n_i = 1$ $\forall i$

$\Rightarrow$ $A \cong D_1 \oplus \cdots \oplus D_k$

Now A is a finite-dim $\mathbb{R}$-alg, hence so are the D_i; but a fin-dim'l division-alg over $\mathbb{R}$ is only $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$.

$\mathbb{H}$ does not have the properties previously stated, so the D_i are $\mathbb{R}$ or $\mathbb{C}$, hence commutative.