ALGEBRA EXAM FEBRUARY 2011

1. Let G be a finite group with a cyclic Sylow 2-subgroup S.

   (a) Show that any element of odd order in $N_G(S)$ centralizes S.

   (b) Show that $N_G(S) = C_G(S)$.

   (c) Give an example to show that (a) can fail if S is abelian.

2. Let G be a finite group with a cyclic Sylow 2-subgroup $S \neq 1$.

   (a) Let $\rho : G \to S_n$ be the regular representation with $n = |G|$. Show that $\rho(G)$ is not contained in A_n.

   (b) Show that G has a normal subgroup of index 2.

   (c) Show that the set of elements of odd order in G form a normal subgroup N and $G = NS$.

3. For a group G and p a prime let $G(p) = \{g \in G | g^p = 1\}$.

   (a) Show that if G is Abelian, then $G(p)$ is a subgroup of G. Give an example to show that $G(p)$ need not be a subgroup in general.

   (b) Let G, H be finitely generated Abelian groups with $G/G(p) \cong H/H(p)$ and $G/G(q) \cong H/H(q)$ for different primes p, q. Show that $G \cong H$.

4. Let R be a prime ring with only finitely many right ideals.

   (a) Show that R is a simple ring.

   (b) Prove that either R is finite or R is a division ring.

5. Let $R = \mathbb{C}[x_1, \ldots, x_n]$ and let J be a nonzero proper ideal of R. Let $A = A(X), B = B(X) \in M_r(R)$ and assume that $\det(A)$ is a product of distinct monic irreducible polynomials in R. Assume that for each $\alpha = (a_1, \ldots, a_n) \in \mathbb{C}_n$, $B(\alpha) \in M_r(\mathbb{C})$ invertible implies that $A(\alpha)$ is invertible. Show that $\det(A)$ divides $\det(B)$ in R.

6. Let L be a splitting field over $\mathbb{Q}$ for $p(x) = x^{10} + 3x^5 + 1$. Let $G = \mathrm{Gal}(L/\mathbb{Q})$.

   (a) Show that G has a normal subgroup of index 2.

   (b) Show that 4 divides $|G|$.

   (c) Show that G is solvable.

Algebra Spring 2011

① G finite group w/ cyclic Sylow 2-s.g. S.

(a) Show any elt of odd order in $N_G(S)$ centralizes S.

(b) Show $N_G(S) = C_G(S)$.

(c) Show (a) can fail if S is assumed abelian rather than cyclic.

---

solution to (a)

Let $g \in N_G(S)$, so $gSg^{-1} = S$. Let $|g|$ odd.

we want to show $gsg^{-1} = s$ for all $s \in S$, i.e. $g \in C_G(S)$.

By Sylow's thm, $n_2 \equiv 1 \pmod 2$ $\Rightarrow$ odd # Sylow 2-s.g.'s.

By considering G acting on its subgroups by conjugation, the # s.g.'s in the orbit of S equals $|G| / \text{size of Stabilizer of } S$ which is $|G|/|N_G(S)|$. we gather $|G|/|N_G(S)| = n_2$ is odd.

Write $|G| = 2^{\alpha} M$, $2 \nmid M$. Hence $2^{\alpha} \mid |N_G(S)|$, by prev paragraph.

Write $|N_G(S)| = 2^{\alpha} m$, m odd. The N/C theorem says

$N_G(S)/C_G(S) < \operatorname{Aut} S \cong \operatorname{Aut}(\mathbb{Z}_{2^\alpha}) \cong (\mathbb{Z}_{2^\alpha})^*$ ← cardinality equals # odds which is $2^{\alpha-1}$.

Hence, $|C_G(S)| = 2^{\beta} m$, $\beta \leq \alpha$.

Now consider $H = \langle g \rangle C_G(S) < N_G(S)$.

Since $H > C_G(S)$, $|H| = 2^{\gamma} m$, $\beta \leq \gamma \leq \alpha$.

We have also $|H| = \dfrac{|\langle g \rangle| \, |C_G(S)|}{|\langle g \rangle \cap C_G(S)|} = \dfrac{|g| m 2^{\beta}}{|\langle g \rangle \cap C_G(S)|} = 2^{\gamma} m$.

So $\dfrac{|g|}{|\langle g \rangle \cap C_G(S)|} = 2^{\gamma - \beta}$. Since $|g|$ is odd, $|\langle g \rangle \cap C_G(S)| = |g|$.

Therefore, $\langle g \rangle < C_G(S)$ and we conclude $g \in C_G(S)$.

$\square$.

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

Return to the previous solution to the point where we wrote $|C_G(S)| = 2^{\beta} m$. Here $\beta \leq \alpha$ and m odd.

From here, we note S abelian $\Rightarrow S < C_G(S)$.

So $2^{\alpha} \mid |C_G(S)|$, hence in fact $\beta = \alpha$.

We conclude immediately $N_G(S) = C_G(S)$ and we also see (a) as a consequence of this; in other words, the last paragraph of the previous solution is unnecessary.

$\square$.

---

solution to (c)

The key to (a) and (b) was that
$|\mathrm{Aut}(S)| = 2^{\alpha}$.

This is true for a cyclic 2-group, but not necessarily for an abelian 2-group.

Indeed, $\mathrm{Aut}(\mathbb{Z}_p^n) \cong GL_n(\mathbb{Z}_p)$

which has order $\prod_{j=0}^{n-1}(p^n - p^j)$.

So e.g. $|\mathrm{Aut}(\mathbb{Z}_2^2)| = 6$.

The sylow 2-s.g. of A_4 is $\mathbb{Z}_2^2$ which is in fact normal (identity + products of disjoint transpositions).

so $N_{A_4}(\mathbb{Z}_2^2) = A_4$, $(123) \in A_4$ has odd order, and

$(123)(12)(34)(132) = (14)(23) \neq (12)(34)$.

$\square$.

(2) G finite group w/ cyclic Sylow 2-s.g. $S \neq 1$.

(a) $\rho : G \to S_n$ regular representation, i.e. $n = |G|$ and G acts on itself by left multiplication. Show $\rho(G) \not\subset A_n$.

(b) Show G has a normal s.g. of index 2.

(c) Show the elements of odd order form a normal s.g. N and $G = NS$.

---

solution to (a) Write $|G| = 2^\alpha m$, $2 \nmid m$.

Let S be multiplicatively generated by x. Since $\ker\rho = 0$, $G < S_n$. We consider the cycle decomposition $\sigma_1 \cdots \sigma_{k_x}$ associated w/ x. For any $g \in G$ we get an orbit as follows: $g \to xg \to x^2 g \to \cdots \to x^{2^\alpha} g = g$. Hence each of the cycles σ_i $(i = 1, \ldots, k_x)$ is of length 2^α. We forget to mention that $x^j g = g$ for $j \in \{0, 1, \ldots, 2^\alpha\}$ iff $j = 0, 2^\alpha$ since $|x| = 2^\alpha$ by assumption. This also tells us $k_x = m$ is odd. So in S_n, x is an odd # of odd cycles (since each cycle has even order) and thus X is odd. so $G \not\subset A_n$. $\square$.

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

Recall $A_n \trianglelefteq S_n$ since $[S_n : A_n] = 2$.

we first show $G A_n = S_n$.

Indeed, since $G \not\subset A_n$, $|G| / |G \cap A_n| \geq 2$.

So $$|GA_n| = \frac{|G||A_n|}{|G \cap A_n|} \geq 2 \cdot \frac{|S_n|}{2} = |S_n|. \checkmark$$

we are done by the Diamond isomorphism theorem, which says since $A_n \trianglelefteq S_n$ and $[S_n : A_n] = 2$ and $GA_n = S_n$ then $[G : G \cap A_n] = 2$, hence $G \cap A_n \trianglelefteq G$.

$$\begin{tikzcd}
 & S_n = GA_n \arrow[dl, no head] \arrow[dr, no head, "2"] & \\
G \arrow[dr, no head, "2"'] & & A_n \arrow[dl, no head] \\
 & G \cap A_n &
\end{tikzcd}$$

$\square$.

solution to (c)

We show $\{\text{odd}^{\text{order}}\text{ elts}\} \equiv N$ is a normal s.g. of G and $G = NS$.

We argue by induction on α.

First a general remark. The same argument used to give a cycle decomp of X in (a) can be used to give a cycle decomp of an arbitrary g: If $|g|$ is given, then g splits as the product of disjoint $|g|$-order cycles, $|G|/|g|$ in total.

Thus we obtain the following dichotomy:

$g \in G$ odd order	$g \in G$ even order	
$\downarrow$ cycle decomp	$\downarrow$ cycle decomp	
	$|g| = 2^{\alpha} m'$	$|g| = 2^{\beta} m'$ $(\beta < \alpha)$
$\underbrace{\text{even}+\text{even}+\cdots+\text{even}}_{\text{even \# times}}$ (or the identity elt)	$\underbrace{\text{odd}+\text{odd}+\cdots+\text{odd}}_{\text{odd \# times}}$	$\underbrace{\text{odd}+\text{odd}+\cdots+\text{odd}}_{\text{even \# times}}$
$\in A_n$	$\notin A_n$	$\in A_n$

To summarize: The odd$^{\text{order}}$ elts of G are the same as the odd-order elts of $A_n \cap G$. The cycle types of g are different depending on whether g is odd-order in A_n, even order in A_n, or even order not in A_n.

Now assume $\alpha = 1$.

Then we see $\{\text{odd-order}\}$ equals all of $A_n \cap G$, which we already know is a normal s.g. of index 2.

Since $X \notin A_n \cap G$, the same argument used in (b) to show $GA_n = S_n$ may be used to show $S(A_n \cap G) = G$.

This concludes the base step.

For the induction step let $\alpha > 1$.

Since $A_n \cap G$ has order $2^{\alpha - 1} m$, we apply the induction hypothesis to $A_n \cap G$ to establish that $N \equiv \{\text{odd-order elts of } A_n \cap G\}$ is a normal <u>subgroup</u> of $A_n \cap G$, and $NS' = A_n \cap G$, where we may take $S' \equiv \langle X^2 \rangle \subset S$.

We already proved that N is simultaneously the set of odd-order elts of G. Since $NS' = A_n \cap G$, $S' \subset S$, and $S(A_n \cap G) = G$, we have $NS = G$.

We will be done if N is normal in G (right now we only know $N \trianglelefteq A_n \cap G \trianglelefteq G$, and normality is not transitive). However, N is a s.g. of G.

Regardless, we know <u>in S_n</u> that the conjugacy classes are determined exactly by cycle type. Since the elts of N, $(A_n \cap G) - N$, and $G - A_n$ are of distinct cycle type, we conclude G conjugates N into itself, hence N is normal. This completes the induction. $\square$

③ G group. p prime. $G(p)=\{g\in G : g^p=e\}$.

(a) Show if G is abelian, then
$G(p)$ is a subgroup of G.
Give an example showing $G(p)$ need not be a s.g. in general.

(b) Let G, H be f.g. abelian groups w/ $G/G(p) \cong H/H(p)$ and $G/G(q) \cong H/H(q)$ for different primes p, q. Show $G \cong H$.

---

solution to (a)

$$(gh)^p = g^p h^p = e. \quad (g^{-1})^p = (g^p)^{-1} = e. \checkmark$$

In $S_3 = \{r, s : r^3 = s^2 = e, \ sr = r^2 s\}$
we have $srsr = srr^2s = e$ and $s^2 = e$
but $(s\, sr)^2 = r^2 \neq e. \checkmark$ $\square$.

solution to (b)

$$G \cong \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{a \text{ times}} \times \underbrace{\mathbb{Z}_q \times \mathbb{Z}_q \times \cdots \times \mathbb{Z}_q}_{b \text{ times}} \times \mathbb{Z}_{p^{\alpha_1}} \times \mathbb{Z}_{p^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p^{\alpha_n}} \times \mathbb{Z}_{q^{\beta_1}} \times \mathbb{Z}_{q^{\beta_2}} \times \cdots \times \mathbb{Z}_{q^{\beta_m}} \times G_1$$

$\mathbb{Z}_p \quad \mathbb{Z}_q \qquad \alpha_i, \beta_i \geqslant 1$

$$H \cong \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{c \text{ times}} \times \underbrace{\mathbb{Z}_q \times \mathbb{Z}_q \times \cdots \times \mathbb{Z}_q}_{d \text{ times}} \times \mathbb{Z}_{p^{\gamma_1}} \times \mathbb{Z}_{p^{\gamma_2}} \times \cdots \times \mathbb{Z}_{p^{\gamma_\ell}} \times \mathbb{Z}_{q^{\varepsilon_1}} \times \mathbb{Z}_{q^{\varepsilon_2}} \times \cdots \times \mathbb{Z}_{q^{\varepsilon_r}} \times H_1 \quad \mathbb{Z}_p \quad \mathbb{Z}_q.$$

$\gamma_i, \varepsilon_i \geqslant 1$

$$G(p) \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p \times \mathbb{Z}_{(p < p^{\alpha_1})} \times \mathbb{Z}_{(p<p^{\alpha_2})} \times \cdots \times \mathbb{Z}_{(p<p^{\alpha_n})} \times 0 \times 0 \times \cdots \times 0 \times 0$$

$\left(\text{e.g. If } \mathbb{Z}_4 = \langle x \rangle \text{ then } \mathbb{Z}_{(2<4)} = \langle x^2 \rangle\right)$

$$G/G(p) \cong \underbrace{\mathbb{Z}_q \times \mathbb{Z}_q \times \cdots \times \mathbb{Z}_q}_{b \text{ times}} \times \mathbb{Z}_{p^{\alpha_1 - 1}} \times \mathbb{Z}_{p^{\alpha_2-1}} \times \cdots \times \mathbb{Z}_{p^{\alpha_n - 1}} \times \mathbb{Z}_{q^{\beta_1-1}} \times \mathbb{Z}_{q^{\beta_2-1}} \times \cdots \times \mathbb{Z}_{q^{\beta_m-1}} \times G_1$$

$\wr\wr$

$$H/H(p) \cong \underbrace{\mathbb{Z}_q \times \mathbb{Z}_q \times \cdots \times \mathbb{Z}_q}_{d \text{ times}} \times \mathbb{Z}_{p^{\gamma_1-1}} \times \mathbb{Z}_{p^{\gamma_2-1}} \times \cdots \times \mathbb{Z}_{p^{\gamma_\ell-1}} \times \mathbb{Z}_{q^{\varepsilon_1-1}} \times \mathbb{Z}_{q^{\varepsilon_2-1}} \times \cdots \times \mathbb{Z}_{q^{\varepsilon_r-1}} \times H_1.$$

In particular, $b = d$.

The info we lose is what a and c are.

It remains to show $a = c$.

Indeed, this is given by the same reason by $G/G(q) \cong H/H(q)$.

$\square$.

(4) R prime ring (w/ 1) and finitely many right ideals.

(a) Show R is simple.

(b) Prove R is finite or R is a division ring.

---

solution to (a) If $I = 0$ we are done. Assume $I \neq 0$.

Recall R being a prime ring means 0 is a prime ideal in the noncommutative sense; namely, if I and J are two-sided ideals and $IJ = 0$, then $I = 0$ or $J = 0$.

Recall the Jacobson radical of R is

$$J = \bigcap_{\substack{M \text{ simple} \\ \text{right } R\text{-module}}} \{a \in R : ma = 0 \ \forall m \in M\}.$$

Since R has finitely many right ideals, let I be a minimal nonzero right ideal (possibly R itself). Then I may be viewed as a nonzero simple right R-module. Let $a \in R$, $ma = 0 \ \forall m \in I$.

So $RI \cdot RaR = RIaR = 0$.

So, since R is a prime ring, either $RI = 0$ or $RaR = 0$. Since $I \neq 0$, $RaR = 0$, so $a = 0$. So $J = 0$.

Since R is clearly right Artinian, R is thus semisimple.

So $R = M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ by A.W.

Each copy of $M_{n_i}(D_i)$ in R is an ideal, and the product of any pair of such ideals is 0 (e.g. $0 = (M_{n_1}(D_1) \times 0 \times \cdots \times 0) \cdot (0 \times M_{n_2}(D_2) \times 0 \times \cdots \times 0)$).

Since R is prime, we must have then $k=1$ and $R = M_n(D)$ is simple. $\square$.

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

Assume R is not finite. So D is infinite.

~~If $n>1$, Any nonzero matrix of the form $\begin{pmatrix} \overline{} \\ 0 \end{pmatrix}$ is a right ideal.~~

~~Since R is infinite, then~~

By the <u>Morita Equivalence</u>, the right ideals of $M_n(D)$ are in 1-to-1 correspondence w/ the submodules of the right free D-module D^n.

If D is infinite and $n>1$, there are infinitely many submodules, as can be seen from the family $\{D \cdot (1, \lambda, 0, \dots, 0)\}_{\text{s.t. } \lambda \in D}$. So $n=1$. $\square$.

(5) Let $R = \mathbb{C}[X_1, \ldots, X_n]$ and let J be a nonzero proper ideal of R. Let $A \equiv A(X)$ and $B \equiv B(X)$ be elts of $M_r(R)$.
Assume $\operatorname{Det} A$ is a product of distinct monic irreducible polys in R.
Assume for each $\alpha = (a_1, \ldots, a_n) \in \mathbb{C}^n$ that $B(\alpha)$ being invertible implies $A(\alpha)$ is invertible.
Show that $\det(A)$ divides $\det(B)$ in R.
(What is J for?)

---

solution

$[B(\alpha)$ invertible $\Longrightarrow A(\alpha)$ invertible$]$ iff

$[\operatorname{Det} B(\alpha) \neq 0 \Longrightarrow \operatorname{Det} A(\alpha) \neq 0]$ iff

$[\operatorname{Det} A(\alpha) = 0 \Longrightarrow \operatorname{Det} B(\alpha) = 0]$ iff

$[\alpha \in V(\operatorname{Det} A(X)) \Longrightarrow \alpha \in V(\operatorname{Det} B(X))]$.

So, setting $a(x) \equiv \operatorname{Det} A(X)$ and $b(x) \equiv \operatorname{Det} B(X)$, we have $V(a(x)) \subset V(b(x))$, hence

$$\begin{array}{ccc} I(V(a(X))) & \supset & I(V(b(x))) \\ \| & & \| \\ \sqrt{(a(x))} & & \sqrt{(b(x))} \ni b(X) \\ \| & & \\ (a(X)) & & \end{array}$$

since $a(x)$ is a product of distinct irreducibles. (I don't think the monic assumption was necessary.)

So $a(X) \mid b(X)$ as desired. $\square$.

---

⑥ Let L be a splitting field over $\mathbb{Q}$ for $p(X) = X^{10} + 3X^5 + 1$. Let $G \equiv \mathrm{Gal}(L/\mathbb{Q})$.

(a) Show G has a normal s.g. of index 2.

(b) Show $4 \mid |G|$.

(c) Show G is solvable.

---

solution to (a)

$p(X) = X^{10} + 3X^5 + 1.$ $\quad y = x^5.$

$p(y) = y^2 + 3y + 1.$ $\quad y = -\frac{3}{2} \pm \frac{\sqrt{5}}{2}.$

$\equiv -\alpha_{\mp} < 0.$

So $X = -\sqrt[5]{\alpha_{\pm}}\,\xi$ where ξ is a primitive 5^{th} root of unity.

Therefore, the splitting field is given by

$L = \mathbb{Q}(\sqrt{5}, \sqrt[5]{\alpha_{\pm}}, \xi).$

By the Galois correspondence, there will exist a subgroup of index 2 (so a normal s.g.) if there is an intermediate subfield of L of index 2 over $\mathbb{Q}$. Indeed, $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}]$ is such a subfield, as $\sqrt{5}$ is the root of $X^2 - 5$ which is irreducible $/\mathbb{Q}$ by Eisenstein. $\square$.

solution to (b)

It suffices to show there is an intermediate field of size 4 over $\mathbb{Q}$, for then the corresponding subgroup has index 4 in G.

Indeed, $[\mathbb{Q}(\zeta):\mathbb{Q}] = 4$ since the minimal poly of ζ is $\Phi_5(x) = x^4+x^3+x^2+x+1$.

$\square$.

---

solution to (c)

Thm: G is solvable iff $\overbrace{\mathbb{Q} \subset L}^{\text{Galois}}$ is solvable

iff $\mathbb{Q} \subset L$ is contained in a radical extension.

But $\mathbb{Q} \subset L$ is a radical extension:

$$\mathbb{Q} \subset \mathbb{Q}(\zeta) \subset \mathbb{Q}(\zeta, \sqrt{5}) \subset \mathbb{Q}(\zeta, \sqrt{5}, \sqrt[5]{\alpha_+}) \subset \mathbb{Q}(\zeta, \sqrt{5}, \sqrt[5]{\alpha_\pm}) = F.$$

$\zeta^5 = 1 \in \mathbb{Q}$ $\quad (\sqrt{5})^2 = 5 \in \mathbb{Q}$ $\quad (\sqrt[5]{\alpha_+})^5 = \alpha_+ = \frac{3}{2} + \frac{\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5})$ $\quad (\sqrt[5]{\alpha_-})^5 = \alpha_- = \frac{3}{2} - \frac{\sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5})$

we conclude G is solvable. $\square$.