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.

$R \cong M_n(D) \cong \mathrm{End}(D^n)$

Artinian many models

Algebra : Spring 2011 :

(1) $|G| < \infty$ & has cyclic Sylow 2-sg. $S \leq G$.

(a) Show that odd order elt in $N_G(S)$ is also in $C_G(S)$

S Sylow 2-sg., hence $|S| = 2^k$ where $|G| = 2^k m$, $2 \nmid m$.

S is cyclic, hence S abelian, hence $S \leq C_G(S) \trianglelefteq N_G(S)$. Recall that $N_G(S)/C_G(S) \hookrightarrow \mathrm{Aut}(S) \cong \mathrm{Aut}(\mathbb{Z}_{2^k}) \cong 2^k - 2^{k-1}$

Therefore $\left| N_G(S)/C_G(S) \right| \mid (2^k - 2^{k-1})$:

Case $k=1$: $\left| N_G(S)/C_G(S) \right| \mid (2-1) \Rightarrow \left| N_G(S)/C_G(S) \right| = 1 \Rightarrow N_G(S) = C_G(S)$

Case $k \geq 1$ $\left| N_G(S)/C_G(S) \right| \mid (2^k - 2^{k-1}) = 2^{k-1}(2-1) = 2^{k-1}$

Hence $\left| N_G(S)/C_G(S) \right|$ is a power of 2, hence $C_G(S)$ must contain all odd-order elts of $N_G(S)$.

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

Since S is abelian, $S \leq C_G(S) \trianglelefteq N_G(S)$, hence $\left| N_G(S)/C_G(S) \right|$ must be odd order ; but it also must be a power of 2 by part (a), hence $\left| N_G(S)/C_G(S) \right| = 1$, hence $N_G(S) = C_G(S)$

(2) $|G| < \infty$ & has cyclic Sylow 2-subgroup $S \leq G$

(a) Letting $\rho: G \to S_n$ be regular rep'n with $|G| = n$, show $\rho(G) \not\subseteq A_n$

G has cyclic sylow 2-sg., hence $|G| = 2^m k$, $2 \nmid k$ & G has an element $x \in G$ of order 2^m.

Under the rep'n $\rho: G \to S_n$, $g \mapsto \gamma_g(h) = gh$, γ_g has fixed pt $\iff g = e$,

hence γ_g consists of $\frac{|G|}{\text{ord}(g)}$ distinct cycles of length $\text{ord}(g)$;

in particular, γ_x is k cycles of length 2^m, i.e. an odd # of even length cycles. Even length cycles have odd # of transpositions hence γ_x is odd # transpositions, hence $\gamma_x \notin A_n$, hence $\rho(G) \not\subseteq A_n$.

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

Since $\rho(G) \not\subseteq A_n$, we have $GA_n \cong S_n$, and therefore

$2 = |S_n / A_n| = |GA_n / A_n| \overset{2^{nd} \text{ iso thm.}}{=} |G / G \cap A_n|$, hence $G \cap A_n$ is isomorphic to an index 2 subgroup of G.

(c) Show that the set of elts of odd order in G form normal s.g. $N \trianglelefteq G$ and $G = NS$:

We showed that a group with cyclic Sylow 2-sg has a subgroup index 2; for G let $H_1 \trianglelefteq G$ be such a sg. Then $|H_1| = 2^{m-1} k$.

Now, since $\exists x \in G$ w/ $\text{ord}(x) = 2^m$, we also have $\text{ord}(x^2) = 2^{m-1}$.

Since γ_{x^2} has $\frac{2^m k}{2^{m-1}} = 2k$ cycles length 2^{m-1}, we have that $\gamma_{x^2} \in A_n$, hence $x^2 \in H$ (since $H_1 = A_n \cap G$). Therefore H_1 has cyclic Sylow 2-sg., hence a subgroup $H_2 \trianglelefteq H_1$ index 2 w/ $|H_2| = 2^{m-2} k$

Applying the same logic we can produce a chain of such subgroups until we arrive at $H_m \leq H_1 \cong G \cap A_n$ order k, hence odd order elements of $|H_1|$; if $g \in G$ odd order then γ_g even # cycles $\Rightarrow \gamma_g \in A_n \Rightarrow g \in A_n$; hence H_m all odd order elts of G.

③ G group, p prime, $G(p) = \{g \in G : g^p = 1\}$

(a) Show that if G abelian, then $G(p)$ subgroup.

$g, h \in G(p) \Rightarrow g^p = 1 = h^p$; note that $g^p g^{-1} = g^{-1} \Rightarrow g^p (g^{-1})^p = (g^{-1})^p$ (1)

Consider gh: $(gh)^p = \underbrace{gh \cdots gh}_{p} = \underbrace{g \cdots g}_{p} \underbrace{h \cdots h}_{p}$ $\Rightarrow g^{-1} \in G(p)$.

$= g^p h^p = 1 \Rightarrow gh \in G(p)$

(b) G, H fin gen abel. grps w/ $G/G(p) \cong H/H(p)$ & $G/G(q) \cong H/H(q)$ for distinct primes $p \neq q$; show $H \cong G$.

G, H fin gen abel grps $\Rightarrow G \cong \mathbb{Z}^N \oplus A_p \oplus A_q \oplus$ (other primes)

$H \cong \mathbb{Z}^M \oplus B_p \oplus B_q \oplus$ (other primes)

where A_p, B_p p-primary part & A_q, B_q the q-primary part.

The summands of $G(p)$, $H(p)$ are p-primary only

$G(q)$, $H(q)$ " q-primary "

So $G(p) \leq A_p$, $H(p) \leq B_p$, $G(q) \leq A_q$, $H(q) \leq B_q$. & thus $G/G(p)$ will have same summands as G in the non-p-primary part, hence:

$$\mathbb{Z}^N \oplus A_p/G(p) \oplus A_q \oplus (\text{others}) = G/G(p) \cong H/H(p)$$

$$\mathbb{Z}^M \oplus B_p/G(p) \oplus B_q \oplus (\text{others}) = H/H(p)$$

$\parallel$ as

Hence $N = M$ and all non-p-primary parts agree. (specifically $A_q \cong B_q$).

On the other hand,

$$\mathbb{Z}^N \oplus A_p \oplus A_q/G(q) \oplus (\text{others}) = G/G(q)$$

$$\mathbb{Z}^M \oplus B_p \oplus B_q/G(q) \oplus (\text{others}) = H/H(q)$$

$\parallel$ as

$\Rightarrow$ agree on all non-q-primary parts; i.e., $A_p \cong B_p$.

$\rightarrow$ therefore, $G \cong H$

④ R prime ring with finitely many right ideals

(a) R is a simple ring:

R prime $\Leftrightarrow$ every pair of ideals $I, J \trianglelefteq R$ with $IJ=(0) \Rightarrow I=0$ or $J=0$.
Since R has finitely many ideals, R is artinian $\Rightarrow J(R)$ nilpotent $\Rightarrow J(R)^n=0$ for some n. Therefore, $J(R)=0$ since R is prime $\Rightarrow R$ is Jacobson semisimple & artinian $\Rightarrow R$ semisimple.
So then by Artin-Wedd, $R \cong B_1 \oplus \cdots \oplus B_k$, B_i simple rings.
Recall the direct summands of R correspond to ideals, and clearly $B_i B_j = 0$ for $i \neq j$, hence one is 0; therefore only one direct summand is nonzero, and hence $R \cong B_i$ for some i, hence R simple.

(b) R finite or division ring

R simple, so by Ar-Wedd, $R \cong M_n(D)$, D division ring.
If $n=1$ then R is a division ring. Suppose $n>1$.
Recall $R \cong M_n(D) \cong \mathrm{End}(D^n)$. These are linear maps, hence they correspond to ideals in D^n (kernels & images), which are just direct sums of ideals in D.

An ideal in D corresponds to one in R, hence finitely many ideals in D, hence finitely many in D^n, hence $\mathrm{End}(D^n)$ is finite, i.e. $|R|<\infty$.

⑤ $R=\mathbb{C}[x_1,\dots,x_n]$ & $J\subsetneq R$. Let $A=A(x)$, $B=B(x)\in M_r(R)$ and assume $\det A(x)=\prod_i p_i(x)$ where p_i monic, distinct, irred/R. Assume for each $\alpha=(a_1,\dots,a_n)\in\mathbb{C}^n$, $B(\alpha)\in M_r(\mathbb{C})$ inv $\Rightarrow A(\alpha)$ inv.

Show: $\det(A)\mid\det(B)$ in R.

For $\alpha\in\mathbb{C}^n$, $B(\alpha)$ inv $\Rightarrow A(\alpha)$ inv means $\det B(\alpha)\neq 0 \Rightarrow \det A(\alpha)\neq 0$, hence $\det A(\alpha)=0\Rightarrow \det B(\alpha)=0$, hence $\mathrm{Var}(\det A(x))\subseteq \mathrm{Var}(\det B(x))$, and therefore $\mathrm{Id}(\mathrm{Var}(\det B(x)))\subseteq \mathrm{Id}(\mathrm{Var}(\det A(x)))$ (order reversing!)

$\Rightarrow \sqrt{(\det B(x))}\subseteq\sqrt{(\det A(x))}$, hence $(\det B(x))\subseteq\sqrt{(\det A(x))}$

Recall $\sqrt{(\det A(x))}=\{f\in\mathbb{C}[x]: f^m\in(\prod_i p_i)\}$

$=\{f\in\mathbb{C}[x]: f^m(x)=g\prod_i p_i \text{ for some } g\}$

But the p_i are irreducible, hence f must already have factors of p_i for each i for $f^m\in(\prod_i p_i)$, hence $f\in(\prod_i p_i)$ to begin with; therefore $\sqrt{(\det A(x))}=(\det A(x))$

$\Rightarrow (\det B(x))\subseteq(\det A(x))\Rightarrow \det B(x)\in(\det A(x))\Rightarrow \det A(x)\mid\det B(x)$

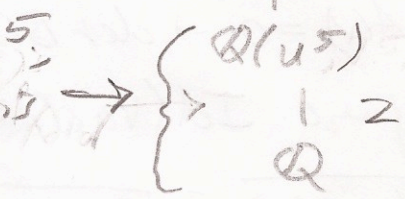
⑥ $L/\mathbb{Q}$ splitting field for $p(x) = x^{10} + 3x^5 + 1$, $G = Gal(L/\mathbb{Q})$

(a) G has normal s.g. index 2:

p has roots $u, \bar{u}$ such that $u^5 = \frac{-3+\sqrt{5}}{2}$, $\bar{u}^5 = \frac{-3-\sqrt{5}}{2}$

Now let $u, \bar{u}, r_3, \dots, r_{10}$ be the roots of p and see that $L = \mathbb{Q}(u, \bar{u}, r_3, \dots, r_{10})$ and consider the tower:

$y^5 + 3y + 1$ is minimal poly^z for u^5, hence $[\mathbb{Q}(u^5) : \mathbb{Q}] = 2$, and a Galois extension



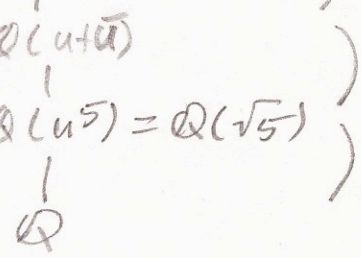
So by FTGT, $Gal(L/\mathbb{Q}(u^5)) \leq G$ of index 2

(b) $4 \mid |G|$:

Consider the element $\sigma \in Gal(L/\mathbb{Q})$ with $\sigma(u) = \bar{u}$

This element has fixed field $\mathbb{Q}(u+\bar{u})$, hence it is in $Gal(L/\mathbb{Q}(u+\bar{u})) \leq Gal(L/\mathbb{Q})$; it is also of order 2, hence $2 \mid [L : \mathbb{Q}(u+\bar{u})] \Rightarrow [L : \mathbb{Q}(u+\bar{u})] = 2l$.

Now consider the tower:



, hence $[L : \mathbb{Q}] = k \cdot 2l \cdot 2 = 4lk$

$\Rightarrow 4 \mid [L : \mathbb{Q}] = |G|$.

(c) G solvable:

Let $H = Gal(L/\mathbb{Q}(u^5)) \trianglelefteq G$ be normal s.g. from part (a) and see $H = Gal(L/\mathbb{Q}(\sqrt{5}))$; now, $L/\mathbb{Q}(u^5)$ is splitting field for $x^5 - u^5$, Clearly $x^5 - u^5$ solvable by radicals, hence $L/\mathbb{Q}(u^5)$ solvable by radicals, hence H is solvable group.

On the other hand, $G/H \cong \mathbb{Z}_2$, hence abelian hence solvable

G/H & H solvable $\Rightarrow$ G solvable.