Kayla Orlinsky

Algebra Exam Spring 2011

Problem 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.

Solution.

(a) Since $S \subset C_G(S) \subset N_G(S)$, (a) and (b) are equivalent. Namely, $[N_G(S) : C_G(S)] = 2n + 1$ for some $n \in \mathbb{N}$.

Therefore, we will prove (b) directly. In fact, we will prove something stronger.

> **Claim 1.** If p is the smallest prime dividing $|G|$ and P is a cyclic Sylow p-subgroup, then $N_G(P) = C_G(P)$.
>
> *Proof.* Let p be the smallest prime dividng $|G|$. Then, since
>
> $$P \trianglelefteq C_G(P) \trianglelefteq N_G(P)$$
>
> we have that
>
> $$[N_G(P) : C_G(P)] = n \qquad \gcd(n, p) = 1.$$
>
> Furthermore, because p is the smallest prime dividing $|G|$, n is only divisible by primes q with $q > p$.
>
> Now, let
>
> $$\begin{aligned} \varphi : N_G(P) &\to \mathrm{Aut}(P) \\ a &\mapsto \sigma_a \end{aligned}$$
>
> be the map of the conjugation action of $N_G(P)$ on P.
>
> Then $C_G(P)$ is clearly the kernel of this action and so by the first isomorphism theorem,
>
> $$N_G(P)/C_G(P) \cong A \subset \mathrm{Aut}(P).$$

Finally, because $P = \langle x \rangle$ is cyclic, we have that the automorphisms of P are exactly the maps $x \mapsto x^k$ for $\gcd(k, p) = 1$. Namely,

$$|\mathrm{Aut}(P)| = p^{l-1}(p-1) \qquad \text{by the Euler Totient Function}$$

assuming that $|P| = p^l$. Since the divisors of this are not greater than p, and $|N_G(P)/C_G(P)|$ has only divisors greater than p, it must be that $|N_G(P)/C_G(P)| = 1$.

Namely,

$$N_G(P) = C_G(P).$$

✌

(b) Since 2 is clearly the smallest prime dividing $|G|$, the claim in (a) applies and we are done.

(c) There is a small example where S is not abelian to show how (b) can fail.

Assume S is a 2-Sylow subgroup and

$$S \cong D_8 = \langle r, s \,|\, s^4 = r^2 = 1, sr = r^{-1}s \rangle.$$

which is non-abelian.

Let $G = S_4$. Since S is non-abelian, $C_G(S)$ does not contain S but $S \subset N_G(S)$ so the two are certainly not equal.

However, in this case, $N_G(S) = S$ and so it contains no elements of odd order.

To contradict (a), we can consider $G = A_4$ which has a normal 2-Sylow subgroup S isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Thus, $N_G(S) = G$ and G certainly contains elements of odd order. However, one can check that $(1\ 2\ 3) \in G$ has odd order and $(1\ 2\ 3) \notin C_G(S)$. In fact, it is true that $C_G(S) = S$.

✌

Problem 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 $G = NS$.

Solution.

(a) The regular representation ρ is the map which sends $g \mapsto \lambda_g$ which is the left multiplication map, namely, $\lambda_g(h) = gh$ for all $h \in G$.

Therefore, by construction, λ_g has no fixed points and, because ρ is a homomorphism, λ_g has order $o(g)$.

> **Claim 2.** λ_g can be represented in S_n as a product of $\frac{|G|}{o(g)}$ cycles each of length $o(g)$.
>
> *Proof.* Let $\lambda_g = \sigma_1 \cdots \sigma_l$ with σ_i disjoint cycles.
>
> Now, because λ_g has no fixed points, the product of the σ_i also have no fixed points.
>
> Next, we note that $\lambda_{g^t} = (\lambda_g)^t$ is non-trival for all $t < o(g)$ and λ_{g^t} also has no fixed points.
>
> Therefore,
> $$(\sigma_1 \cdots \sigma_l)^t = \sigma_1^t \cdots \sigma_l^t$$
> has no fixed points for all $t < o(g)$ and so, letting k_i be the length of σ_i for all i, we get that $k_i \geq o(g)$ for all i.
>
> However, since $o(\lambda_g) = o(g) = \text{lcm}(\text{distinct cycle lengths})$, we get that $k_i \leq o(g)$ for all i.
>
> Therefore, $k_i = o(g)$ for all i.
>
> Finally, the only way for there to be no fixed points is if all n integers are expressed in some σ_i. Therefore,
> $$n = \sum_{i=1}^{l} k_i = l o(g) \implies l = \frac{n}{o(g)}.$$
>
> Thus, λ_g can be expressed as $\frac{n}{o(g)}$ cycles each of length $o(g)$. ✌

Let $S = \langle x \rangle$ since it is cyclic, $o(x) = 2^k$ for $|S| = 2^k$.

From the claim, $\rho(x) = \lambda_x$ can be written as a product of $\frac{n}{2^k}$ cycles, each of length 2^k.

Since S is a 2-Sylow subgroup, $\frac{n}{2^k}$ is odd, and so λ_x is a product of an odd number of even length cycles. Since cycles of even length are expressed as an odd number of transpositions, λ_x is a product of an odd number of transpositions, an odd number of times.

Therefore, $\rho(x) = \lambda_x \notin A_n$ and so $\rho(G) \not\subset A_n$.

(b) Since $\rho(G) \not\subset A_n$ by (a), and since A_n is normal in S_n, we have that

$$A_n \subsetneq \rho(G)A_n \subset S_n.$$

However, since $[S_n : A_n] = 2$, we have that A_n is maximal and so $\rho(G)A_n = S_n$.

Now, because

$$\frac{|S_n|}{|A_n|} = 2$$

and by the first isomorphism theorem,

$$\rho(G)A_n/A_n \cong \rho(G)/(\rho(G) \cap A_n)$$

so we get that

$$2 = \frac{|S_n|}{|A_n|} = \frac{|\rho(G)A_n|}{|A_n|} = \frac{|\rho(G)|}{|\rho(G) \cap A_n|}.$$

Thus, because $\rho(G) \cap A_n \subset \rho(G)$ is a subgroup, we have that $\rho(G)$ has a subgroup of index 2.

And since $\rho(G) \cong G$, G has a subgroup of index 2 which is normal because 2 is the smallest prime dividing $|G|$. (For a proof see **Spring 2010, Claim 1**)

(c) Let N be the set of elements of odd order in G.

Now, let $|G| = n = 2^k m$. Then, because G by (b), we can let K_1 be a normal subgroup of index 2. Then $|K_1| = 2^{k-1}m$.

If we can show that K_1 has a cyclic Sylow 2-subgroup, then (b) will apply again and K_1 will have a normal subgroup of index 2.

Let $S = \langle x \rangle$. Then x has order 2^k by assumption. Therefore, x^2 has order 2^{k-1} since

$$(x^2)^{2^{k-1}} = x^{2 \cdot 2^{k-1}} = x^{2^k} = e$$

so $o(x^2)|2^{k-1}$ and also clearly $o(x^2) \geq 2^{k-1}$.

So, we claim that $\langle x^2 \rangle$ is a copy of a Sylow 2-subgroup of K_1.

However, this follows since $\rho(K_1) \cong \rho(G) \subset A_n$ and since $\rho(x^2) = \lambda_{x^2} \in A_n$.

This is because λ_{x^2} can be represented as a product of $\frac{|G|}{o(x^2)} = \frac{2^k m}{2^{k-1}} = 2k$ cycles of length 2^{k-1}. Since even length cycles are odd and the product of two odd cycles is even, we get that λ_{x^2} is even.

Therefore, $x^2 \in K_1$ and so K_1 has a cyclic Sylow 2-subgroup.

Thus, (b) applies and so we repeat to obtain a chain

$$K_k \trianglelefteq K_{k-1} \trianglelefteq \cdots \trianglelefteq K_1 \trianglelefteq G$$

with $|K_j| = 2^{k-j}m$.

Therefore, $|K_k| = m$ and is a subgroup of G containing only odd order elements. Let $K_k = N$.

Finally, $G \cong K_1\langle x \rangle$ since $x \notin K_1$ and K_1 is of minimal index and so is of maximal order.

Similarly, $K_1 \cong K_2\langle x^2 \rangle$. Thus,

Therefore,

$$G \cong Ne\langle x^{2^{k-1}} \rangle \cdots \langle x^2 \rangle \langle x \rangle = NS.$$

Note that this follows from order arguments and uses no assumptions that N is normal in G. Namely, if $|HK| = |G|$, then $HK = G$ regardless of whether or not H or K is normal.

Now, we simply note that if $n \in N$ with order t for t odd, then

$$(x^l n x^{-l})^t = x^l n^t x^{-l} = x^l e x^{-l} = e$$

and so $x^l n x^{-l}$ has order dividing t, and so namely, it has odd order.

Therefore, $x^l n x^{-l} \in N$ for all l, so $N \subset N_G(S)$.

Now, let $g \in G$. Then since $G = NS$, $g = n_0 x^l$ for some $n_0 \in N$ and some l.

Therefore,

$$gng^{-1} = n_0 x^l n x^{-l} n_0^{-1} = n_0 n' n_0^{-1} \in N$$

since $x^l \in S$ and $N \subset N_G(S)$.

Therefore, N is normal in G.

✌

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

(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 $G \cong H$.

Solution.

(a) Assume G is abelian. Then let $a, b \in G(p)$. Then $(ab^{-1})^p = a^p b^{-p} = 1$ since G is abelian and so $ab^{-1} \in G(p)$.

Let $G = S_3$. Then
$$G(2) = \{1, (1\ 2), (1\ 3), (2\ 3)\}$$
which is clearly not a subgroup since
$$(1\ 2)(2\ 3) = (1\ 2\ 3) \notin G(2).$$

(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.

By the fundamental theorem of abelian groups, we can write
$$\begin{aligned} G &\cong \mathbb{Z}^m \oplus \mathbb{Z}_{p_1}^{\alpha_1} \oplus \cdots \oplus \mathbb{Z}_{p_k}^{\alpha_k} \\ H &\cong \mathbb{Z}^n \oplus \mathbb{Z}_{q_1}^{\beta_1} \oplus \cdots \oplus \mathbb{Z}_{q_l}^{\beta_l} \end{aligned}$$

Then, if $a \in G(p)$, then $o(a)|p$ and so namely, either $a = 1$ or $a \in \mathbb{Z}_p$.

If $G(p) = 1$ and $H(p) = 1$, then we are done.

Assume $G(p) \neq 1$. Then $G(p) \cong \mathbb{Z}_p^t$ for some $t > 0$

$\boxed{H(p) = 1}$ Then $p_i = p$ for some i. WLOG, say $p_1 = p$. Then
$$\begin{aligned} G/G(p) &\cong H \\ \mathbb{Z}^m \oplus \mathbb{Z}_p^{\alpha_1 - t} \oplus \cdots \oplus \mathbb{Z}_{p_k}^{\alpha_k} &\cong \mathbb{Z}^n \oplus \mathbb{Z}_{q_1}^{\beta_1} \oplus \cdots \oplus \mathbb{Z}_{q_l}^{\beta_l} \end{aligned}$$

Therefore, with possible reindexing, $m = n$, $k = l$, and $\alpha_i = \beta_i$ for all $i \neq 1$, and $\alpha_1 - t = \beta_1$. Note that this can be proved using projection maps, or by counting arguments.

Now, regardless of what $G(q)$ and $H(q)$ are, we will get a contradiction.

If $G(q)$ and $H(q)$ are both trivial, then $H \cong G$ so $H \ncong G/G(p)$. If $G(q) \neq 1$, then $G/G(q) \cong H/H(q)$, however, this will imply, after possibly reindexing, that $p_1 = q_1$ and $\alpha_1 = \beta_1$.

However, this contradicts the above, that $\alpha_1 - t = \beta_1$.

$\boxed{H(p) \neq 1}$ Then $H(p) \cong \mathbb{Z}_p^s$ for $s > 0$ so, after possibly reindexing, we can take $q_1 = p$.

$$G/G(p) \cong H/H(p)$$
$$\mathbb{Z}^m \oplus \mathbb{Z}_p^{\alpha_1 - t} \oplus \cdots \oplus \mathbb{Z}_{p_k}^{\alpha_k} \cong \mathbb{Z}^n \oplus \mathbb{Z}_p^{\beta_1 - s} \oplus \cdots \oplus \mathbb{Z}_{q_l}^{\beta_l}$$

Thus, $m = n$, $k = l$, $\alpha_i = \beta_i$ for all $i \neq 1$, and $\alpha_1 - t = \beta_1 - s$.

Now, we repeat with $G(q)$ and $H(q)$, which both cannot be trivial by the same argument as earlier, to get that $\alpha_1 = \beta_1$ and we are done.

Problem 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.

Solution.

(a) A prime ring is a ring satisfying: if $a, b \in R$, and $arb = 0$ for all $r \in R$ implies $a = 0$ or $b = 0$. Alternatively, if I, J are both ideals of R and $IJ = 0$, then $I = 0$ or $J = 0$.

Now, since R has only finitely many right ideals, it is right artinian and so $J(R)$ is nilpotent.

However, if $(J(R))^n = 0$, then either $J(R) = 0$ or $(J(R))^{n-1} = 0$ because R is prime. Recursively, we get that $J(R) = 0$.

Thus, by Artin-Wedderburn, R is semisimple and so

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

for D_i division rings.

Now, recall that the matrix rings $M_{n_i}(D_i)$ represent simple submodules of R and further note that the submodules of R (considered as an R-module) are exactly the ideals of R as a ring.

Finally, because the $M_{n_i}(D_i)$ are simple submodules, they correspond exactly to minimal ideals I_i of R. Namely, $M_{n_i}(D_i) \cong R/M_i$ for some maximal ideal $M_i \subset R$.

Therefore, because I_iI_j is an ideal for all i, j and $I_iI_j \subsetneq I_i$ which is minimal, we get that $I_iI_j = 0$ for all $i \neq j$.

However, because R is prime, this forces $I_i = 0$ or $I_j = 0$.

Recursively, we lose all but one of the matrix rings in the decomposition and so

$$R \cong M_n(D) \qquad \text{which is simple.}$$

(b) If R is finite we are done.

Assume R is not finite. From (a),

$$R \cong M_n(D)$$

for some division ring D. Note that because R is assumed infinite, D is infinite.

However, the right ideals of $M_n(D)$ correspond exactly to the right D-submodules of the free D-module D^n.

If $n > 1$, then D^n has infinitely many submodules. For example, $D^n(1, a, 0, ..., 0) \cong D \oplus Da$ is a non-trivial proper submodule for all $a \in D$ (of which there are infinitely many because D must be infinite).

This implies that R has infinitely many right ideals, which is a contradiction.

Thus, $n = 1$ and so $R \cong D$.

✌

Problem 5. Let $R = \mathbb{C}[x_1, ..., x_n]$ 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 $\alpha = (a_1, ..., a_n) \in \mathbb{C}$, $B(\alpha) \in M_r(\mathbb{C})$ invertible implies that $A(\alpha)$ is invertible. Show that $\det(A)$ divides $\det(B)$ in R.

Solution. if whenever $B(\alpha)$ is invertible $A(\alpha)$ is also invertible, then whenever $\det(B) \neq 0$, $\det(A) \neq 0$.

Thus, if $\det(A) = 0$, $\det(B) = 0$. Therefore, if $I = (\det(A))$, every $\alpha \in (V(I))$ also satisfies $\det(B)(\alpha) = \det(B(\alpha)) = 0$.

Therefore, by Nullstellenzat's Part II, there exists an $n > 0$ such that $\det(B)^n \in I$.

Therefore, there exists $f(X) \in R$ such that $\det(B)^n = f(X)\det(A)$. Since $\det(A)$ consists of a product of distinct monic irreducible polynomials, say $\det(A) = g_1(X) \cdots g_k(X)$, for each $g_i(X) | \det(A)$, $g_i(X) | \det(B)^n$. Inductively, by the irreducibility of g_i, we get that $g_i(X) | \det(B)$ for all i.

Therefore, $\det(A) | \det(B)$ in R. ✌

Problem 6. Let L be the 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.

Solution.

(a) Let $u = x^5$. Then $p(x) = x^{10} + 3x^5 + 1 = u^2 + 3u + 1$. Thus, using the quadratic formula,

$$u = \frac{-3 \pm \sqrt{9-4}}{2} = \frac{-3 \pm \sqrt{5}}{2} \notin \mathbb{Q}.$$

Therefore, $u^2 + 3u + 1$ is irreducible over $\mathbb{Q}$ and so $p(x)$ is irreducible over $\mathbb{Q}$. We can note also that $p(x)$ is separable since $x^5 = \frac{-3\pm\sqrt{5}}{2}$, yields no repeated roots. Namely, L is indeed a Galois extension over $\mathbb{Q}$.

Now, if $\alpha = \sqrt[5]{\frac{-3+\sqrt{5}}{2}}$ and $\beta = \sqrt[5]{\frac{-3-\sqrt{5}}{2}}$, then the roots of $p(x)$ are exactly, $\alpha\xi^i$ and $\beta\xi^j$ where ξ is a 5^{th} root of unity and for $i, j \in \{1, ..., 5\}$.

Therefore,

$$G = \mathbb{Q}(\sqrt[5]{\alpha}, \sqrt[5]{\beta}, \xi).$$

Now, by the Galois Correspondence Theorem, the normal subgroups of G correspond exactly to the Galois extensions of $\mathbb{Q}$ contained in L, and furthermore, there is an $N \trianglelefteq G$ with $[G : N] = 2$ if and only if there is a $K \subset L$ such that $[L : K] = \frac{|G|}{2}$, or alternatively, if and only if there is a $K \subset L$ with $[K : \mathbb{Q}] = 2$. Since

$$\alpha^5 - \beta^5 = \frac{-3+\sqrt{5}}{2} - \frac{-3-\sqrt{5}}{2} = \frac{2\sqrt{5}}{2} = \sqrt{5} \in L$$

we have that $\mathbb{Q}(\sqrt{5}) \subset L$.

Since $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$, there exists a subgroup $N \subset G$ with $[G : N] = 2$ which is normal since 2 is the smallest prime dividing $|G|$. *(To see a proof of this see* ***Spring 2010, Problem 2, Claim 1****).*

Show that G has a normal subgroup of index 2.

(b) Since ξ satisfies $x^4 + x^3 + x^2 + x + 1$, $[\mathbb{Q}(\xi) : \mathbb{Q}] = 4$ and so G has a subgroup of index 4.

Namely, $4||G|$.

(c) G is solvable if and only if L is contained in a radical extension of $\mathbb{Q}$.

However, L is a radical extension of $\mathbb{Q}$.

Recall that a radical extension is one in which $\mathbb{Q} = K_1 \subset K_2 \subset \cdots \subset K_n = L$ with $K_i = K_{i-1}(\alpha_i)$ for all i for α_i satisfying that there exists t with $\alpha_i^t \in K_{i-1}$.

Therefore, since

$$\mathbb{Q} \subset \mathbb{Q}(\xi) \subset \mathbb{Q}(\sqrt{5}, \xi) \subset \mathbb{Q}(\sqrt{5}, \alpha, \xi) \subset \mathbb{Q}(\sqrt{5}, \alpha, \beta, \xi) = L$$

and

$$\begin{aligned}
(\beta)^5 &= 3 - \alpha^5 \in \mathbb{Q}(\sqrt{5}, \alpha, \xi) \\
(\alpha)^5 &= \frac{-3 + \sqrt{5}}{2} \in \mathbb{Q}(\sqrt{5}, \xi) \\
(\sqrt{5})^2 &= 5 \in \mathbb{Q}(\xi) \\
(\xi)^5 &= 1 \in \mathbb{Q}
\end{aligned}$$

we have that L is a radical extension.

Therefore, G is solvable.

✌