Kayla Orlinsky

Algebra Exam Fall 2014

Problem 1. Let G be a group of order 56 having at least 7 elements of order 7. Let S be a Sylow 2-subgroup of G.

(a) Prove that S is normal in G and $S = C_G(S)$.

(b) Describe the possible structures of G up to isomorphism. (Hint: How does an element of order 7 act on the elements of S.)

Solution.

(a) Since by Sylow $n_7|8$ and $n_7 \equiv 1 \mod 7$, $n_7 = 1, 8$. Because G has at least 7 elements of order 7, $n_7 \neq 1$ so $n_7 = 8$.

Thus, because Sylow 7-subgroups are cyclic in G and they are conjugates, G actually has $6 \cdot 8 = 48$ elements of order 7.

Since $56 - 48 = 8$, G can have only 7 elements of even order.

Thus, G has one Sylow 2-subgroup, S.

Now, by assumption G is non-abelian (its Sylow 7-subgroup is not normal). Thus, $C_G(S) \neq G$.

Now, because S is normal, $C_G(S)$ will also be normal in G. if $a \in G$, $x \in C_G(S)$, $s \in S$, then

$$\begin{aligned} axa^{-1}s(axa^{-1})^{-1} &= axa^{-1}sax^{-1}a^{-1} \\ &= axs_0x^{-1}a^{-1} \qquad a^{-1}sa = s_0, \\ &= as_0a^{-1} \\ &= s \qquad s = as_0a^{-1} \end{aligned}$$

Thus, $axa^{-1} \in C_G(S)$.

Therefore, if $|C_G(S)| = 56/2 = 28$, then $C_G(S)$ will be normal in G.

However, in $C_G(S)$, $n_7 \equiv 1 \mod 7$, $n_7|4$ so $C_G(S)$ has a normal Sylow 7-subgroup. However, normal Sylow subgroups of normal subgroups are normal in the whole group (see **Fall 2011: Problem 5 Claim 3**). This contradicts that G has 8 Sylow 7-subgroups.

If $|C_G(S)| = 14$, then again $C_G(S)$ has a normal Sylow 7-subgroup and so again, this would force G to have a normal Sylow 7-subgroup.

Finally, $|C_G(S)| \neq 7$ because again, $C_G(S)$ is normal in G.

Therefore, $|C_G(S)|$ has even order so $C_G(S) \subset S$.

Thus, $C_G(S) = Z(S)$ and so it cannot be trivial since S is a p-group and so has non-trivial center by the class equation.

Let $s \in S$ not be in $C_G(S)$. Then there exists $a, b \in S$ with $a \neq b$ and $sas^{-1} = b$. If $a \in C_G(S)$ then

$$b = sas^{-1} = sas^{-1}a^{-1}a = ss^{-1}a = a$$

which is a contradiction. Similarly, $b \notin C_G(S)$. Note that clealry $s \neq a$ and $s \neq b$.

However, this implies that there are an odd number of elements not in $C_G(S)$ which is impossible since $C_G(S) \subset S$ and so has even order.

To see this, note that so far we have found 3 total elements not in $C_G(S)$ and since $C_G(S)$ has even order, there must exist at least one more $c \in S$ such that $c \notin C_G(S)$ and c is distinct from a and b.

However, scs^{-1} cannot be a or b, else we would get that c is one of the a or b. Namely, if $scs^{-1} = b$ then $scs^{-1} = sas^{-1}$ so $c = a$.

Therefore, there must exist some d such that $scs^{-1} = d$, where $d \neq a, b, c, s$. Furthermore, by the same reasoning as before, $d \notin C_G(S)$. Else

$$c = s^{-1}ds = s^{-1}dsd^{-1}d = s^{-1}sd = d$$

which contradicts that $c \notin C_G(S)$.

However, we now have 5 distinct elements not in $C_G(S)$. Repeating we obtain a contradiction, that $C_G(S)$ is trivial.

Finally, $C_G(S) = Z(S) = S$ and so S is abelian.

(b) Since S is abelian,

$$S \cong \mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2^3.$$

This will give three possible structures for G.

Note that by the recognizing semi-direct products theorem, $G \cong P_7 S$ where P_7 is a Sylow 7-subgroup.

$\boxed{\varphi : P_7 \to \text{Aut}(\mathbb{Z}_8)}$ Let

$$\varphi : P_7 \to \text{Aut}(\mathbb{Z}_8) \cong \mathbb{Z}_8^\times \cong \mathbb{Z}_{8-2} \cong \mathbb{Z}_6$$

Since there are no elements of order 7 in $\text{Aut}(\mathbb{Z}_8)$, only the trivial homomorphism is well defined. Since this would define an abelian structure on G, this cannot lead to a possible structure for G.

$\boxed{\varphi : P_7 \to \text{Aut}(\mathbb{Z}_4 \times \mathbb{Z}_2)}$ Let $\varphi : P_7 \to \text{Aut}(\mathbb{Z}_4 \times \mathbb{Z}_2)$.

First, if $\sigma : \mathbb{Z}_4 \times \mathbb{Z}_2 \to \mathbb{Z}_4 \times \mathbb{Z}_2$ is an automorphism, one can check that to ensure the kernel of σ is trivial, we only have the following choices for σ :

$$\begin{array}{lcl} \sigma(1,0) = (1,0) & \text{and} & \sigma(0,1) = (0,1) \\ \sigma(1,0) = (1,1) & \text{and} & \sigma(0,1) = (0,1) \\ \sigma(1,0) = (3,0) & \text{and} & \sigma(0,1) = (0,1) \\ \sigma(1,0) = (3,1) & \text{and} & \sigma(0,1) = (0,1) \\ \sigma(1,0) = (3,1) & \text{and} & \sigma(0,1) = (1,0) \\ \sigma(1,0) = (3,0) & \text{and} & \sigma(0,1) = (1,0) \\ \sigma(1,0) = (1,1) & \text{and} & \sigma(0,1) = (1,0) \\ \sigma(1,0) = (1,0) & \text{and} & \sigma(0,1) = (1,0) \end{array}$$

Namely, $\text{Aut}(\mathbb{Z}_4 \times \mathbb{Z}_2)$ has order 8 and so again, there are no elements of order 7 for φ to map.

$\boxed{\varphi : P_7 \to \varphi : P_7 \to \text{Aut}(\mathbb{Z}_2^3)}$ $\varphi : P_7 \to \text{Aut}(\mathbb{Z}_2^3) \cong GL_3(\mathbb{F}_2)$. Since

$$|GL_3(\mathbb{F}_2)| = (2^3-1)(2^3-2)(2^3-2^2) = 7 \cdot 6 \cdot 4 = 2^3 \cdot 3 \cdot 7$$

Therefore, there exists a non-trivial homomorphism φ under which we can define the semi-direct product structure for G.

Now, any φ must map P_7 to a Sylow 7-subgroup of $\text{Aut}(\mathbb{Z}_2^3)$. Since Sylow subgroups are conjugates, any two different homomorphisms φ_1, φ_2 will have conjugate images. Namely, they will generate isomorphic semi-direct products.

Thus, there is only one possible group G with non-normal Sylow 7-subgroup.

To actually write down a presentation for G, we must find an element of order 7 in $\text{Aut}(\mathbb{Z}_2^3)$.

Let $S \cong \langle a, b, c\rangle$ and $P_7 \cong \langle d\rangle$.

After some effort, one obtains that the automorphism of S defined by $a \mapsto b$, $b \mapsto bc$, $c \mapsto a$ defined an automorphism of order 7.

Therefore, we get the following multiplication for

$$G \cong \mathbb{Z}_2^3 \times_\varphi \mathbb{Z}_7$$

,

$$G \cong \langle a, b, c, d \,|\, a^2 = b^2 = c^2 = d^7 = 1, dad^{-1} = b, dbd^{-1} = bc, dcd^{-1} = a\rangle.$$

This is the only possible structure for G.

✌

Problem 2. Show that a finite ring with no nonzero nilpotent elements is commutative.

Solution. Let R be a finite ring with no nonzero nilpotent elements.

Let $r \in J(R)$. Then $1 - r$ is invertible in R because $J(R)$ is quasi-regular.

Now, because R is artinian (it is finite), we have a decreasing chain

$$(r) \supset (r^2) \supset \cdots$$

which must terminate after a finite number of steps. Namely, $(r^n) = (r^m)$ for all $n \geq m$.

However, $r^m = ar^{m+1}$ for some $a \in R$. Thus,

$$r^m(1 - ar) = 0.$$

Since $ar \in J(R)$, $1 - ar$ has an inverse so $r^m = 0$. Namely, r is nilpotent.

Since $r \in R$, it must be that $r = 0$.

Thus, $J(R) = 0$.

Therfore, by Artin Wedderburn, $R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$ for some division rings D_i. Note that because R is finite, D_i must be finite, and since finite division rings are fields, $D_i \cong \mathbb{F}_{q_i}$ a field of q_i elements.

However, since R has no nonzero nilpotent elements and

$$A = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 \\ & \vdots & \ddots & \vdots & \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \end{bmatrix}$$

is a nilpotent matrix over any field (any division ring really), $n_i = 1$ for all i.

Thus, $R \cong \mathbb{F}_{q_1} \oplus \cdots \oplus \mathbb{F}_{q_k}$ and so it is commutative. ✌

Problem 3. If $R = M_n(\mathbb{Z})$, and A is an additive subgroup of R, show that as additive subgroups $[R : A]$ is finite if and only if $R \otimes_{\mathbb{Z}} \mathbb{Q} = A \otimes_{\mathbb{Z}} \mathbb{Q}$.

Solution.

$\boxed{\Longrightarrow}$ Assume $[R : A] = m < \infty$. Then for all $X \in R/A$, with $X \neq 0$ (in other words for $X \notin A$), $mX = 0 \in R/A$ since R/A is a finite group, (in other words, $mX \in A$).

Therefore for all $X \in R$ with $X \notin A$, and all $q \in \mathbb{Q}$, $X \otimes mq = mX \otimes q \in A \otimes_{\mathbb{Z}} \mathbb{Q}$ and clearly if $X \in A$, then $X \otimes q \in A \otimes_{\mathbb{Z}} \mathbb{Q}$ so $R \otimes_{\mathbb{Z}} \mathbb{Q} = A \otimes_{\mathbb{Z}} \mathbb{Q}$.

$\boxed{\Longleftarrow}$ Note that $R \cong \mathbb{Z}^{n^2}$ and so R is a finitely generated free module over a PID ($\mathbb{Z}$ is a PID).

Therefore, A is also a free finitely generated $\mathbb{Z}$-module so $A \cong \mathbb{Z}^m$ for some m since submodules of free module over PIDs are also free and additive subgroups are submodules.

Therefore, if $R \otimes_{\mathbb{Z}} \mathbb{Q} = A \otimes_{\mathbb{Z}} \mathbb{Q}$ then $\mathbb{Z}^{n^2} \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Z}^m \otimes_{\mathbb{Z}} \mathbb{Q}$, so of course $n^2 = m$.

Therefore, $[R : A] < \infty$ since if $[R : A] = \infty$ then there exists i, j so there are an infinite number of possible values in the ij^{th} entry of every matrix of R/A. Namely, $X \in R/A$ can have any infinite number of possible values in its ij^{th} entry.

However, then R/A has an isomorphic copy of $\mathbb{Z}$ in it, and so namely, it has rank ≥ 1. However, this is not possible since rank of R/A is rank$(R)-$rank$(A) = n^2 - n^2 = 0$.

Thus, $[R : A] < \infty$. ✌

Problem 4. Let R be a commutative ring with 1, n a positive integer and $A_1, ..., A_k \in M_n(R)$. Show that there is a noetherian subring S of R containing 1 with all $A_i \in M_n(S)$.

Solution. First, we note that since $\varphi : \mathbb{Z} \to R$ defined by $\varphi(1) = 1_R$ has kernel which is an ideal of $\mathbb{Z}$, namely an additive subgroup, so either $\mathbb{Z}$ or $\mathbb{Z}_n$ has an isomorphic copy in R.

Therefore, we can consider $S \cong \mathbb{Z}[A_1, ..., A_k]$, the subring generated by the entries of the A_i. Then since S is a finitely generated algebra over a PID, it is a noetherian subgring of R and $M_n(S)$ contains all the A_i.

✌

Problem 5. Let $R = \mathbb{C}[x, y]$. Show that there exists a positive integer m such that $((x + y)(x^2 + y^4 - 2))^m$ is in the ideal $(x^3 + y^2, y^3 + xy)$.

Solution. This question is from **Fall 2012: Problem 3**, thus we provide the same proof here that we did there.

By Nullstellensatz, if $(x+y)(x^2+y^4-2)$ satisfies every point $(a, b) \in V(x^3+y^2, y^3+xy)$, then $(x+y)(x^2+y^4-2) \in \sqrt{I}$ and there exists an integer m such that $((x+y)(x^2+y^4-2))^m \in (x^3 + y^2, y^3 + xy)$.

Thus, we compute $V(x^3 + y^2, y^3 + xy)$.

If $x^3+y^2 = 0$ and $y^3+xy = 0$ simultaneously, then $x^3y+y^3-y^3-xy = 0$ so $x^3y-xy = 0$ so $xy(x^2 - 1) = 0$. Thus, we have $x = 0, 1, -1$ or $y = 0$. This gives the following points $(0, 0), (1, i), (1, -i), (-1, 1), (-1, -1) \in V(x^3 + y^2, y^3 + xy)$.

Since $(x + y)(x^2 + y^4 - 2)$ $(0, 0), (-1, 1)$ immediately satisfy $(x + y)$, we need only check $(x^2 + y^4 - 2)$.

Since $1^2 + (i)^4 - 2 = 1 + 1 - 2 = 0$, $1^2 + (-i)^4 - 2 = 0$, $(-1)^2 + (-1)^4 - 2 = 2 - 2 = 0$, we have by Nullstellensatz that $(x + y)(x^2 + y^4 - 2)$ is satisfied by every point $(a, b) \in V(x^3 + y^2, y^3 + xy)$, so $(x + y)(x^2 + y^4 - 2) \in \sqrt{I}$ and there exists an integer m such that $((x + y)(x^2 + y^4 - 2))^m \in (x^3 + y^2, y^3 + xy)$. ✌

Problem 6. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree $n \geq 5$. Let L be the splitting field of f and let α be a zero of f. Given that $[L : \mathbb{Q}] = n!$, prove that $\mathbb{Q}[\alpha^4] = \mathbb{Q}[\alpha]$.

Solution. Since f is irreducible and $\mathbb{Q}$ is characteristic 0, f is separable.

Thus, $L/\mathbb{Q}$ is Galois.

Now, since $G = \mathrm{Gal}(L/\mathbb{Q})$ embeds into S_n (since f has degree n), $G \cong S_n$ for $n \geq 5$.

Now, by **Spring 2014: Problem 5**, for $n \geq 5$, S_n has no subgroups of index $2 < [S_n : H] < n$.

Now, we simply note that by the fundamental theorem of Galois Theory, subfields of L over $\mathbb{Q}$ correspond exactly to subgroups of $G = S_n$.

Specifically, subgroups H of S_n correspond to subfields $\mathbb{Q} \subset K \subset L$ satisfying that $|H| = [L : K]$ and $[S_n : H] = [K : \mathbb{Q}]$.

Now, $L/\mathbb{Q}(\alpha^4)$ corresponds to a subgroup H of S_n such that

$$[S_n : H] = [\mathbb{Q}(\alpha^4) : \mathbb{Q}].$$

Thus, $[\mathbb{Q}(\alpha^4) : \mathbb{Q}] \geq n$ or $[\mathbb{Q}(\alpha^4) : \mathbb{Q}] \leq 2$.

Now, because α has minimal polynomial $f(x)$ over $\mathbb{Q}$, thus we have that

$$[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^4)] = \frac{[\mathbb{Q}(\alpha) : \mathbb{Q}]}{[\mathbb{Q}(\alpha^4) : \mathbb{Q}]} = \frac{n}{[\mathbb{Q}(\alpha^4) : \mathbb{Q}]}.$$

Therefore, $[\mathbb{Q}(\alpha^4) : \mathbb{Q}] \leq n$.

Next, $[\mathbb{Q}(\alpha^4) : \mathbb{Q}] \neq 1$ since then α would have a minimal polynomial of degree 4 over $\mathbb{Q}$, but the minimal polynomial of α has degree 5.

Now, if $[\mathbb{Q}(\alpha^4) : \mathbb{Q}] = 2$ then $H = A_n$ and α^4 has minimal polynomial $x^2 + ax + b$ for $a, b \in \mathbb{Q}$. However, then $\alpha^4 = \frac{-a \pm \sqrt{a^2 - 4b}}{2a}$ and so the minimal polynomial of α over $\mathbb{Q}$, which is $f(x)$, is solvable by radicals, which is not possible since S_n is not solvable for $n \geq 5$.

Thus, $[\mathbb{Q}(\alpha^4) : \mathbb{Q}] = n$ and so $[\mathbb{Q}(\alpha) : \mathbb{Q}(\alpha^4)] = 1$. Namely, $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha^4)$. ✌