Algebra I - Homework 3

Pablo Sánchez Ocal

September 23th, 2016

Exercise 1

Consider a group G and $n \in \mathbb{Z}$, we want to prove that $\langle\{g^n : g \in G\}\rangle$ is a normal subgroup of G.

Take any $h \in G$, we note that $h^{-1}g^n h = (h^{-1}gh)^n \in \langle\{g^n : g \in G\}\rangle$ since we have multiple cancellations $h^{-1}h = e$. This means that for a general $g_1^{\pm n} \cdots g_k^{\pm n}$ with $g_i \in G$ (not necessarily different) for $i \in \{1, \ldots, k\}$:

$$h^{-1}(g_1^{\pm n} \cdots g_k^{\pm n})h = (h^{-1}g_1^{\pm n}h)(h^{-1} \cdots h)(h^{-1}g_k^{\pm n}h) = (h^{-1}g_1^{\pm 1}h)^n \cdots (h^{-1}g_k^{\pm 1}h)^n,$$

which is a multiplication of elements in $\langle\{g^n : g \in G\}\rangle$ and thus $h^{-1}g_1^{\pm n} \cdots g_k^{\pm n}h \in \langle\{g^n : g \in G\}\rangle$ and this is a normal subgroup.

Exercise 2

Given a group G, let $G' = \langle \{g^{-1}h^{-1}gh : g, h \in G\} \rangle$ the commutator subgroup of G.

1. G' is a normal subgroup: for any $f \in G$ and $h \in G'$, we note that $f^{-1}hf = h(h^{-1}f^{-1}hf) \in G'$ since $h \in G' \leq G$ and $h^{-1}f^{-1}hf \in G'$ by definition.

2. G/G' is abelian: take $gG', hG' \in G/G'$ for $g, h \in G$, we want to prove that $ghG' = hgG'$. For this, it is necessary and sufficient that $g^{-1}h^{-1}gh \in G'$, which is true by definition of G'.

3. Let $N \triangleleft G$, then G/N is abelian if and only if $N \supset G'$.

   $\Longleftarrow$) Let $N \supset G'$, then $G/N \leq G/G'$ meaning that G/N must be abelian since and any subgroup of an abelian group is abelian.

   $\Longrightarrow$) For G/N to be abelian means that $ghN = hgN$ for every $g, h \in G$, thus by construction of the cosets $(hg)^{-1}gh = g^{-1}h^{-1}gh \in N$, meaning that $G' \subset N$.

Exercise 3

We know that cycles of length three generate A_n. Prove that $S_n' = A_n$. We recall that $S_n' = \langle\{\sigma^{-1}\tau^{-1}\sigma\tau : \sigma, \tau \in S_n\}\rangle$.

$\subseteq$) Note that for every $\sigma, \tau \in S_n$:

$$\text{sig}(\sigma^{-1}\tau^{-1}\sigma\tau) = \text{sig}(\sigma^{-1})\text{sig}(\tau^{-1})\text{sig}(\sigma)\text{sig}(\tau) = \text{sig}(\sigma)\text{sig}(\tau)\text{sig}(\sigma)\text{sig}(\tau) = 1$$

thus since A_n is the group of even permutations, $\sigma^{-1}\tau^{-1}\sigma\tau \in A_n$ and $S_n' \subset A_n$.

$\supseteq$) Consider (ijk) a cycle of length three ($i, j, k \in \{1, \dots, n\}$), consider $\sigma = (kj)$, $\tau = (ji)$, then:

$$\sigma^{-1}\tau^{-1}\sigma\tau = (jk)(ij)(kj)(ji) = (ijk)$$

thus every generator of A_n belongs to S_n, in particular $A_n \subset S_n'$.

Exercise 4

For G a group, denote $Z(G) = \{g \in G : gh = hg \, \forall h \in G\}$.

1. $Z(G)$ is normal: for every $h \in G$ and every $g \in Z(G)$ we have $h^{-1}gh = h^{-1}hg = g \in Z(G)$, thus $Z(G)$ is normal.

2. Suppose $G/Z(G)$ is cyclic, prove G is abelian: suppose $G/Z(G) = \langle gZ(G) \rangle$ for certain $g \in G$. Now for every $h, f \in G$ we have $hZ(G) = g^n Z(G)$, $fZ(G) = g^m Z(G)$ for certain $n, m \in \mathbb{Z}$. This implies that $h^{-1}g^n, f^{-1}g^m \in Z(G)$. Applying this to g, we obtain that $(h^{-1}g^n)g = g(h^{-1}g^n)$, $(f^{-1}g^m)g = g(f^{-1}g^m)$ and then $h^{-1}g = gh^{-1}$, $f^{-1}g = gf^{-1}$ thus $hg = gh$, $fg = gf$. Applying $h^{-1}g^n \in Z(G)$ to $f^{-1}g^m$, we obtain that $(h^{-1}g^n)(f^{-1}g^m) = (f^{-1}g^m)(h^{-1}g^n)$ and by the above, this means $g^{n+m}h^{-1}f^{-1} = g^{n+m}f^{-1}h^{-1}$ thus $hf = fh$ and G is abelian.

Exercise 5

We consider the Heisenberg group H (with respect to multiplication) of all upper triangular matrices with integer coefficients.

We first note that if we take $A, B \in H$, then:

$$AB = \begin{pmatrix} 1 & x_1 & y_1 \\ 0 & 1 & z_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x_2 & y_2 \\ 0 & 1 & z_2 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x_2 + x_1 & y_2 + x_1 z_2 + y_1 \\ 0 & 1 & z_2 + z_1 \\ 0 & 0 & 1 \end{pmatrix}$$

and:

$$BA = \begin{pmatrix} 1 & x_2 & y_2 \\ 0 & 1 & z_2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x_1 & y_1 \\ 0 & 1 & z_1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x_1 + x_2 & y_1 + x_2 z_1 + y_2 \\ 0 & 1 & z_1 + z_2 \\ 0 & 0 & 1 \end{pmatrix}.$$

1. Describe $Z(H)$: By the above, when we multiply $B \in H$ and $A \in Z(H)$, the condition $AB = BA$ is true if and only if $x_1 z_2 = x_2 z_1$. This imposes that $x_1 = 0$, $z_1 = 0$ (in A), since if any of them is not zero, then we can easily find B with $AB \neq BA$ (just take $x_2 \neq x_1$, $z_2 \neq z_1$, $x_2 \neq z_2$). Thus:

   $$A = \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

   but since:

   $$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^a = \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \text{ we have } Z(H) = \left\langle \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle.$$

2. Show that $H/Z(G)$ is abelian: take $A, B \in H$, we just want to prove that $ABZ(H) = BAZ(H)$, or equivalently $(BA)^{-1}AB \in Z(H)$. For this, note that:

   $$AB \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{x_2 z_1} = \begin{pmatrix} 1 & x_2 + x_1 & y_2 + x_1 z_2 + y_1 + x_2 z_1 \\ 0 & 1 & z_2 + z_1 \\ 0 & 0 & 1 \end{pmatrix}$$

   and:

   $$BA \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{x_1 z_2} = \begin{pmatrix} 1 & x_1 + x_2 & y_1 + x_2 z_1 + y_2 + x_1 z_2 \\ 0 & 1 & z_1 + z_2 \\ 0 & 0 & 1 \end{pmatrix},$$

   thus:

   $$(BA)^{-1}AB = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{x_1 z_2} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-x_2 z_1} \in Z(H).$$

3. To describe the commutator $H' = \langle \{A^{-1}B^{-1}AB : A, B \in H\} \rangle$, note that by the point above for any $A, B \in H$ we have $A^{-1}B^{-1}AB \in Z(H)$, thus $H' \subset Z(H)$. Moreover:

$$(BA)^{-1}AB = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{1 \cdot 1} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^{-0 \cdot 1} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

by just taking $x_1 = 1$, $z_2 = 1$ and $x_2 = 0$ in the point above. Thus $Z(H) \subset H'$ and we have the equality $H' = Z(H)$.

Exercise 6

Consider G a group of order p^2 for p prime, we show that G is abelian. Note that since $Z(G)$ is a normal subgroup of G, we must have $|Z(G)| \in \{p^2, p, 1\}$.

1. If $|Z(G)| = p^2$ then $Z(G) = G$ and obviously G is abelian.

2. If $|Z(G)| = p$, then $|G/Z(G)| = 2$, thus $G/Z(G)$ must be cyclic and by Problem 3.4 we have that G is abelian.

3. We will prove that $|Z(G)| \neq 1$, that is, the center cannot be trivial. For this, suppose it is and we have $|Z(G)| = 1$. Consider the action of G on itself:

$$\begin{array}{rccc} \psi & : & G \times G & \longrightarrow & G \\ & & (g,x) & \longmapsto & g^{-1}xg \end{array}$$

for which the orbit of the identity element is $\mathcal{O}_e = \{e\} = Z(G)$ (since the identity commutes with everybody and $Z(G)$ is a subgroup of one element).

We now want to prove that $|\mathcal{O}_x| = [G : G_x] = |G|/|G_x|$ (where $G_x = \{g \in G : g(x) = x\}$ is the stabilizer of $x \in G$, and because $|G|$ is finite and $G_x \leq G$, then $|G_x|$ is finite too). For this, consider:

$$\begin{array}{rccc} \varphi & : & G/G_x & \longrightarrow & \mathcal{O}_x \\ & & gG_x & \longmapsto & g(x) \end{array}$$

with $g(x) = g^{-1}xg$ the conjugation, and note that:

$$\begin{aligned} gG_x = hG_x &\iff h^{-1}g \in G_x \iff h^{-1}g(x) = x \\ &\iff g(x) = h(x) \iff \varphi(gG_x) = \varphi(hG_x). \end{aligned}$$

which proves that φ is well defined and it is injective. For the surjectivity, note that any $y \in \mathcal{O}_x$ can by definition be written as $g(x) = y$ for some $g \in G$, and thus $\varphi(gG_x) = g(x) = y$. This proves that $|\mathcal{O}_x|$ divides $|G|$, thus $|\mathcal{O}_x| \in \{p^2, p, 1\}$.

We know that the orbits $\mathcal{O}_x$ for $x \in G$ partition G, that is, an element belongs to one and only one orbit. Thus we have that $|G| = |\mathcal{O}_{x_1}| + \cdots + |\mathcal{O}_{x_n}|$ for some $x_1, \ldots, x_n \in G$. Since $\mathcal{O}_e = \{e\}$, we need one of the elements to be e, take $x_1 = e$ without loss of generality. Then:

$$|G| = |\mathcal{O}_e| + |\mathcal{O}_{x_2}| + \cdots + |\mathcal{O}_{x_n}| = |Z(G)| + |\mathcal{O}_{x_2}| + \cdots + |\mathcal{O}_{x_n}| = 1 + |\mathcal{O}_{x_2}| + \cdots + |\mathcal{O}_{x_n}|$$

but $|G| = p^2$, on the right hand side we can only use elements in $\{p^2, p, 1\}$ and $p^2 - 1$ is not divisible by p^2 or p. This means that there is at least another element $x_k \neq e$ with $|\mathcal{O}_{x_k}| = 1$, that is, $g^{-1}x_k g = x_k$ for every $g \in G$, that is, $x_k \in Z(G)$. This is a contradiction with the hypothesis that $|Z(G)| = 1$, and thus $|Z(G)| \neq 1$, as desired.