# Algebra I, Fall 2016

Solutions to Problem Set 2

2. There is a surjective map $\phi : H_1 \times H_2 \to H_1H_2$ which sends $(a, b)$ to $ab$. Two elements $(a_1, b_1)$ and $(a_2, b_2)$ are mapped to the same element if $a_1b_1 = a_2b_2$, so $a_2^{-1}a_1 = b_2b_1^{-1}$ and since the right hand side is in $H_2$ and the left hand side is in $H_1$, $c := a_2^{-1}a_1 = b_2b_1^{-1} \in H_1 \cap H_2$ and $(a_2, b_2) = (a_1c^{-1}, cb_1)$. Conversely for every element $x \in H_1 \cap H_2$,

$$\phi(a_1, b_1) = \phi(a_1x^{-1}, xb_1).$$

So for every $(a, b)$ in $H_1 \times H_2$, there are $|H_1 \cap H_2|$ elements in $H_1 \times H_2$ which are mapped to $\phi(a, b)$, so

$$|H_1H_2| = \frac{|H_1 \times H_2|}{|H_1 \cap H_2|}.$$

3. The number of distinct conjugates of $H$ is equal to $[G : N_G(H)] = \frac{|G|}{|N_G(H)|}$ Since $|N_G(H)| \geq |H|$ and since all the conjugates of $H$ contain the identity element of the group we have

$$|\bigcup_g gHg^{-1}| \leq 1 + (\frac{|G|}{|N_G(H)|})(|H| - 1) \leq 1 + (\frac{|G|}{|H|})(|H| - 1) = |G| + 1 - \frac{|G|}{|H|} < |G|$$

since $H$ is a proper subgroup.

4. $G$ acts on $N$ by conjugation. For $x \in N$, the orbit of $x$ has only one element if and only if $gxg^{-1} = x$ for all $g$, that is if $gx = xg$ for all $g$, that is if $x \in Z(G)$. If the orbit of $x$ has more than one element then $|O_x|$ is a divisors of $p^n$ as it is equal to $\frac{|G|}{|G_x|}$, and is therefore a multiple of $p$. We have

$|N| =$ (number of orbits of size 1)+(the sum of the sizes of distinct orbits of size $> 1$).

The number in the second parenthesis is a multiple of $p$ and so is the left hand side of the equation, so the number in the first parenthesis should be also a multiple of $p$ , so $|N \cap Z(G)|$ should be a multiple of $p$, but there are $p$ elements in $N$, so $N \subset Z(G)$.

5. Let $F_g$ be the number of elements in $X$ which are fixed by $G$, and assume to the contrary that $F_g \geq 1$ for all $g$ in $G$. We have proved that the number of distinct orbits for the action of $G$ on $X$ is equal to

$$\frac{1}{|G|} \sum_{g \in G} F_g.$$

Since the action is transitive, there is only one orbit, so we have

$$|G| = \sum_{g \in G} F_g = F_e + \sum_{e \neq g \in G} F_g = |X| + \sum_{e \neq g \in G} F_g \geq |X| + (|G| - 1)$$

which is not possible since $|X| \geq 2$.

6. Consider the map $\phi : G \to S_G$ which sends $g$ to the permutation $\phi_g$ where

$$\phi_g(x) = gx.$$

Clearly this is a group homomorphism:

$$\phi_{g_1 g_2}(x) = (g_1 g_2)x = g_1(g_2 x) = \phi_{g_1}(\phi_{g_2}(x)) = \phi_{g_1} \circ \phi_{g_2}(x).$$

The kernel of $\phi$ consists of all $g$ such that $\phi_g(x) = x$ for all $x$, that is $gx = x$ for all $x$, so $g = e$.

7. As we have seen in class, there is a group homomorphism $\phi : G \to \mathrm{Aut(G)}$ such that $\phi(g)$ is the automorphism which sends $x$ to $gxg^{-1}$ for every $x \in G$. The kernel of $\phi$ is exactly the center of the group, $Z(G)$.

By the first isomorphism theorem, $G/Z(G)$ is isomorphic to the image of $\phi$ which is a subgroup of a cyclic group, and is therefore cyclic. So $G/Z(G)$ is cyclic. Assume $G/Z(G)$ is generated by the left cost $aZ(G)$. Then every element of $G$ is of the form $a^r z$ for some $z \in Z(G)$ and some integer $r$. So to show the group is commutative it is enough to show that any two elements of the form $a^r z_1$ and $a^s z_2$ commute when $z_1$ and $z_2$ are in the center of the group. We have

$$a^r z_1 a^s z_2 = a^r a^s z_1 z_2 = a^r a^s z_2 z_1 = a^s a^r z_2 z_1 = a^s z_2 a^r z_1.$$