Group Theory, 2016

Exercise sheet 8 (solutions)

Exercise 1. (a) The multiplicative identity is 1 and we know from Algebra 2B that the multiplication in $\mathbb{H}$ is associative. The inverse of $\pm i$ is $\mp i$. Similarly the inverses of $\pm j$ and $\pm k$ are $\mp j$ and $\mp k$. Also 1 and -1 are self inverses. It remains to see that Q is closed with respect to the multiplication and this one sees from inspection (using $k = i \cdot j = -j \cdot i, i = j \cdot k = -k \cdot j$ and $j = k \cdot i = -i \cdot k$).

(b) Let H be a subgroup of Q. By Lagrange we have that $|H|$ divides $|Q| = 8$ and thus $|H| \in \{1, 2, 4, 8\}$. If $|H| = 1$ then $H = \{1\}$ and if $|H| = 8$ then $H = Q$ which are of course both normal in Q. If $|H| = 4$ then $[Q : H] = 2$ and we know from lectures that $H \trianglelefteq Q$. It remains to deal with the case when $|H| = 2$ but then all the elements of H have order 1 or 2, by Lagrange. Inspection shows that there are only two such elements in Q, namely 1 and -1 and these elements commute with everything in Q. Hence $H = \{1, \ -1\}$ is normal in Q. We have already listed the subgroups of order $1, 2$ and 8. These are $\{1\}$, $\{1, -1\}$ and Q. Any group of order 4 must contain some of the $\pm i, \pm j, \pm k$ but these are all elements of order 4. Hence the groups of order 4 are

$$\langle i \rangle = \{i, -1, -i, 1\}, \ \langle j \rangle = \{j, -1, -j, 1\}, \ \langle k \rangle = \{k, -1, -k, 1\}.$$

Exercise 2. Let xG be any G-orbit of X. By the orbit stabilizer theorem we have that $|xG| = [G : G_x]$ and thus a power of p. Suppose that

$$X = x_1 G \cup x_2 G \cup \cdots \cup x_r G$$

is a partion of X into disjoint orbits. If all the orbits would have order greater than 1 they would all have order divisible by p. In that case we would get the contradiction that $|X|$ is divisible by p. Hence one of the orbits $x_i G$ has only one element which means that x_i is fixed by all $g \in G$.

Exercise 3. By Theorem 5.1, G has a non-trivial centre $Z(G)$. Then, as $|G/Z(G)|$ divides p^2, $|G/Z(G)|$ is either 1 or p. As any group of prime order is cyclic it follows that $G/Z(G)$ is cyclic and thus by Exercise 2 from Sheet 2, we know that G is abelian. From our classification of finite abelian groups we then know that we have two groups of order p^2, namely $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

Exercise 4. We have that N is invariant under conjugation by elements from G. We thus have that N is a G-set with right multiplication $n * g = n^g$. Clearly the stabilizer of n under this action is $C_G(n)$ and so the Orbit-Stabilizer Theorem gives us that

$$|n^G| = [G : C_G(n)]$$

where $n^G = n * G = \{n^g : \ g \in G\}$. Now write N as a disjoint union of G-orbits, say

$$N = n_1^G \cup \cdots \cup n_r^G \cup n_{r+1}^G \cup \cdots \cup n_{r+s}^G$$

where the first r orbits are those that have only one element and the remaining ones have more than 1 element (and thus order divisible by p as the order is $[G : C_G(n_{r+i})]$ that divides $|G|$ and is thus a power of p). As the number of elements in N is divisible by p it follows that r is divisible by p and therefore $Z(G) \cap N = \{n_1, \, n_2, \, \ldots, n_r\}$ has at least $p \geq 2$ elements.

In particular if $|N| = p$ then as $|N \cap Z(G)| > 1$ and divides $|N| = p$, we must have $|N \cap Z(G)| =$

$p = |N|$ and thus $N \cap Z(G) = N$. In this case we thus have that $N \leq Z(G)$. $\square$

Exercise 5. Firstly notice that $a_p = (a_1 \cdots a_{p-1})^{-1}$ and thus $|X| = |H|^{p-1}$ which is a number divisible by p.

Since $(a_1, \ldots, a_p)\mathrm{id} = (a_1, \ldots, a_p)$ and

$$((a_1, \ldots, a_p)\alpha)\beta = (a_{(1)\alpha\beta}, \ldots, a_{(p)\alpha\beta}) = (a_1, \ldots, a_p)(\alpha\beta)$$

it is clear that X is a G-set. Let $(a_1, \ldots, a_p)G$ be any G-orbit of X. By the orbit stabilizer theorem we have that

$$|(a_1, \ldots, a_p)G| = [G : G_{(a_1,\ldots,a_p)}|$$

which is either p or 1. Notice also that $(a_1, \ldots, a_p)$ has orbit of size 1 if and only if $a_1 = a_2 = \cdots = a_p$.

Now suppose that

$$X = (a_1, \ldots, a_p)G \cup \cdots \cup (z_1, \ldots, z_p)G$$

is a partion of X into G-orbits. Now suppose that we have r orbits with single element. The rest of the orbits then have p elements. As $|X|$ is divisble by p it follows that p divides r. But as $(e, \cdots, e) \in X$ and whose orbit is of size 1, we have that $r \geq 1$. Hence $r \geq p \geq 2$ and there exists some $e \neq a \in G$ such that $(a, \cdots, a) \in X$. In other words there exists $a \in H$ such that $a^p = 1$. This finishes the proof.