Algebra 2 Assignment 1

BM Corser

November 17, 2017

1. (a) Let α represent a clockwise rotation of $\frac{\pi}{2}$ about the origin and β represent a particular reflection. Now the Cayley table of Dih(8) can be written

	e	α	α^2	α^3	β	$\alpha\beta$	$\alpha^2\beta$	$\alpha^3\beta$
e	e	α	α^2	α^3	β	$\alpha\beta$	$\alpha^2\beta$	$\alpha^3\beta$
α	α	α^2	α^3	e	$\alpha\beta$	$\alpha^2\beta$	$\alpha^3\beta$	β
α^2	α^2	α^3	e	α	$\alpha^2\beta$	$\alpha^3\beta$	β	$\alpha\beta$
α^3	α^3	e	α	α^2	$\alpha^3\beta$	β	$\alpha\beta$	$\alpha^2\beta$
β	β	$\alpha^3\beta$	$\alpha^2\beta$	$\alpha\beta$	e	α^3	α^2	α
$\alpha\beta$	$\alpha\beta$	β	$\alpha^3\beta$	$\alpha^2\beta$	α	e	α^3	α^2
$\alpha^2\beta$	$\alpha^2\beta$	$\alpha\beta$	β	$\alpha^3\beta$	α^2	α	e	α^3
$\alpha^3\beta$	$\alpha^3\beta$	$\alpha^2\beta$	$\alpha\beta$	β	α^3	α^2	α	e

   (b) The set of elements that commute with every other element in Dih(8) is $\{\alpha^2, e\}$ this can be observed in the Cayley table above by noticing that for each of these elements, both the row and column for that element contain the same elements in the same order.

   (c) The subgroups of Dih(8) are the trivial and identity subgroups $\{e\}$ and Dih(8), the four 2-subgroups formed by every reflecting element and the identity, $\{e, \alpha^n\beta\}$ for $0 \leq n \leq 3$, the commutative 2-subgroup $\{e, a^2\}$, the 4-subgroup containing the identity and all rotation elements $\{e, \alpha, \alpha^2, \alpha^3\}$ and finally the 4-subgroup containing $\{e, \alpha^2, \alpha\beta, \alpha^3\beta\}$.

   By Lagrange, the order of any subgroup $H \leq$ Dih(8), $|H|$ must divide |Dih(8)|. So there aren't any 3- or 5-subgroups because neither 3 or 5 divide 8.

   Now, a subgroup must use a subset of Dih(8) and we needn't consider subsets of size 3 or 5.

   There can only be one 1-subgroup, $\{e\}$, so there aren't any more of those.

   There aren't any 2-subgroups beyond those already mentioned, because none of the non-reflecting 2-subsets $\{e, \alpha^n\}$ with $1 \leq n \leq 3$ have closure.

   There aren't any more 4-subgroups because (with the expection of the subgroup $\{e, \alpha^2, \alpha\beta, \alpha^3\beta\}$) any subgroup that has a combination

of reflections and rotations doesn't have closure.

There can only be one 8-subgroup, Dih(8), so there aren't any more of those either.

2. Let $k, l \in K$ and 1_K be the identity element of K. Since $K \leq G$, we know

$$k, l, kl \in G.$$

Because $f : G \to H$, certainly $f(k), f(l), f(kl) \in H$ and $f(K) \subseteq H$.

Since f is a homomorphism, we know that $f(ab) = f(a)f(b)$ and therefore

$$f(kl) = f(k)f(l) \in H, \tag{1}$$

and, if 1_H is the identity element of H,

$$f(1_K) = 1_H. \tag{2}$$

The fact that f is a homomorphism also tells us that $f(a^{-1}) = f(a)^{-1}$ and since $k^{-1} \in K$ it is also true that

$$f(k)^{-1} \in H. \tag{3}$$

Due to the facts that $K \leq G$ and that f is a homomorphism, it is also true that if $j \in K$,

$$f((jk)l) = f(jk)f(l) = f(j)f(k)f(l) = f(j)f(kl) = f(j(kl)). \tag{4}$$

Therefore $f(K)$ is closed (1), has an identity element 1_H (2), has inverses (3) and is associative (4). Hence, $f(K) \leq H$.

3. (a) $V_4 = \{e, a, b, c\}$ such that
$ab = ba = c$,
$ac = ca = b$,
$bc = cb = a$ and
$a^2 = b^2 = c^2 = e$.

Let f be an automorphism on V_4. Because f is a homomorphism, $f(e) = e$, that is, f fixes e.

Because of this and because of the definition of V_4, any permutation on $\{e, a, b, c\}$ where e is fixed is an automorphism of which there are $\Big|\{a, b, c\}\Big|! = 6$.

(b) There is clearly one automorphism on $\mathbb{Z}_4$, that is the identity automorphism $\theta : \mathbb{Z}_4 \to \mathbb{Z}_4$ where $\theta(n) = n$ for all $n \in \mathbb{Z}_4$. There is also the automorphism $\vartheta : \mathbb{Z}_4 \to \mathbb{Z}_4$, which for $n \in \mathbb{Z}_4$

$$\vartheta(n) = \begin{cases} \vartheta(0) = 0 \\ \vartheta(1) = 3 \\ \vartheta(2) = 2 \\ \vartheta(3) = 1 \end{cases}$$

(c) From the starting point that an automorphism f on $\mathbb{Z}_p$ must be a permutation statisfying the homomorphism property $f(ab) = f(a)f(b)$ for all $a, b \in \mathbb{Z}_p$, I wrote a short C++ program to test permutations for this property. The code is available at the following URL
`https://git.io/vFSef`.
and its output for $p \in \{5, 7, 11\}$ was

```
Z_p, p = 5 has 24 permutations
  ( 0 1 2 3 4 )
  ( 0 2 4 1 3 )
  ( 0 3 1 4 2 )
  ( 0 4 3 2 1 )
Z_p, p = 5 has 4 automorphisms

Z_p, p = 7 has 720 permutations
  ( 0 1 2 3 4 5 6 )
  ( 0 2 4 6 1 3 5 )
  ( 0 3 6 2 5 1 4 )
  ( 0 4 1 5 2 6 3 )
  ( 0 5 3 1 6 4 2 )
  ( 0 6 5 4 3 2 1 )
Z_p, p = 7 has 6 automorphisms

Z_p, p = 11 has 3.6288e+06 permutations
  ( 0 1 2 3 4 5 6 7 8 9 10 )
  ( 0 2 4 6 8 10 1 3 5 7 9 )
  ( 0 3 6 9 1 4 7 10 2 5 8 )
  ( 0 4 8 1 5 9 2 6 10 3 7 )
  ( 0 5 10 4 9 3 8 2 7 1 6 )
  ( 0 6 1 7 2 8 3 9 4 10 5 )
  ( 0 7 3 10 6 2 9 5 1 8 4 )
  ( 0 8 5 2 10 7 4 1 9 6 3 )
  ( 0 9 7 5 3 1 10 8 6 4 2 )
  ( 0 10 9 8 7 6 5 4 3 2 1 )
Z_p, p = 11 has 10 automorphisms
```

The program suggested a clear result, namely that there are $p - 1$ many automorphisms f on $\mathbb{Z}_p$. By inspecting the output, it is easy to observe (for those primes tested) that for all $\{g : \langle g \rangle = \mathbb{Z}_p\}$ and $a \in \mathbb{Z}_p$

$$f(a) = \begin{cases} f(0) = 0 \\ f(a) = g^a \end{cases}$$

Because f is a permutation, it is a bijection. Also the homomorphism

condition $f(ab) = f(a)f(b)$ for all $a, b \in \mathbb{Z}_p$ holds

$$\begin{aligned} f(ab) &= f(a)f(b) \\ f(a \oplus b) &= f(a) \oplus f(b) \\ g^{a \oplus b} &= g^a \oplus g^b \\ (a \oplus b) \times g &= (a \times g) \oplus (b \times g) \text{(due to group operation)} \\ &= (a \oplus b) \times g \end{aligned}$$