Group Theory, 2016
Exercise sheet 1 (solutions)

Exercise 1. Suppose we have some group multiplication on G. Let $x \in G$. As the map $u \mapsto xu$ is bijective (with inverse $u \mapsto x^{-1}u$), we know that each row of the multiplication table must have three different elements. Similarly as the map $u \mapsto ux$ is bijective (with inverse $u \mapsto ux^{-1}$), we know that each column of the multiplication table must have three different elements. We will make use of this 'Sudoko property'. As e is the identity element we get the partial multiplication table

	e	a	b
e	e	a	b
a	a		
b	b		

Now there is only one possible 'sudoku completion' of this table. We must have that $a \cdot b$ is different from $a \cdot e = a$ as well as $e \cdot b = b$ and this forces $a \cdot b = e$. Now there is only one slot left in the 2nd row and thus $a \cdot a = b$. Finally there is only one slot left in both column 2 and 3 and we must have $b \cdot a = e$ and $b \cdot b = a$. So we have shown that there is a unique multiplication table. Notice that there is a group with three elements (namely $(\mathbb{Z}_3, +)$) and thus there is a group multiplication on $\{e, a, b\}$ and we have seen that it is unique. $\square$.

Exercise 2. The roots of the polynomial are $x_1 = -1/2 + (\sqrt{3}/2)i, x_2 = -1/2 - (\sqrt{3}/2)i$ and $x_3 = 1$. As we saw in lectures, any automorphism $\phi : \mathbb{C} \to \mathbb{C}$ must fix 1 and thus the only candiate for the Galois group apart from id is the permutation that swaps x_1 and x_2. In fact there is an automorphism that does this namely $z \mapsto \bar{z}$. So the Galois group is $G = \{\text{id},\ (1\ 2)\}$. $\square$.

Exercise 3. Let r be the 90 degrees rotation counterclockwise around the centre. The permutations $(1\ 2\ 3\ 4)$, $(1\ 3)(2\ 4)$ and $(1\ 4\ 3\ 2)$ correspond to r, r^2 and r^3. Apart from these and id there are also reflections in the four symmetry axes of the square namely

$$(1\ 4)(2\ 3),\ (1\ 2)(3\ 4),\ (1\ 3),\ (2\ 4)$$

One can convince oneself that these are the only 8 permutations in the symmetry group of the square. (One way of arguing is to consider what an isometry does with $\{x_1, x_3\}$. The resulting two points must have the same distance and this can only happen if the set $\{x_1, x_3\}$ is fixed or mapped to $\{x_2, x_4\}$. So any isometry either fixes the sets $\{x_1, x_3\}$ and $\{x_2, x_4\}$ or swaps them. Both these cases lead to further division as the there are two possibilites for the value of each of x_1 and x_2. Hence for each case we have 4 possibilites and thus at most 8 in total).

Exercise 4. It remains to show that e is also a left identity and that every right inverse is also a left inverse.

Step 1. Every right inverse is also a left inverse.

To see this let b a right inverse of a. Let also c be a right inverse of ba. Now using the fact that b is a right inverse of a and e is a right identity, we have

$$baba = b(ab)a = (be)a = ba.$$

Then using the fact that c is a right inverse of ba and again that e is a right identity we see from this that

$$e = bac = babac = bae = ba.$$

Hence b is also a left inverse of a.

Step 2. The right identity e is also a left identity.

To see this let $a \in G$ and let b be a right invese of a. By Step 1 we know that b is also a left inverse. Then, using the fact that e is a right identity, we have

$$ea = (ab)a = a(ba) = ae = a.$$

Hence e is also a left identity. $\square$

Exercise 5. First we show that $(\mathbb{Z}^G, +)$ is an abelian group. As the addition in $\mathbb{Z}$ is both commutative and assocative the same is true of $\mathbb{Z}^G$. Let $\bar{0} \in \mathbb{Z}^G$ be the map that maps every group element in G to 0. Clearly $\bar{0}$ is an additive identity in $\mathbb{Z}^G$. If $\phi \in \mathbb{Z}^G$ and $\bar{\phi} \in \mathbb{Z}^G$ is the map given by $\bar{\phi}(g) = -\phi(g)$ then $[\phi + \bar{\phi}](g) = 0$ and thus $\phi + \bar{\phi} = \bar{0}$ that shows that $\bar{\phi}$ is an additive inverse of ϕ.

Next we show that ϵ is a muliplicative identity and that the multiplication in R is associative. Let $\phi \in \mathbb{Z}^G$. Then

$$[\phi \cdot \epsilon](g) = \sum_{\substack{f,h \in G \\ fh=g}} \phi(f)\epsilon(h) = \phi(g)\epsilon(1_G) = \phi(g)$$

that shows that $\phi \cdot \epsilon = \phi$. Similarly $\epsilon \cdot \phi = \phi$ and we have shown that ϵ is a multiplicatve identity. For the associative law let $\alpha, \beta, \gamma \in \mathbb{Z}^G$ let $\phi = \alpha \cdot \beta$ and $\psi = \beta \cdot \gamma$. Then, using the fact that $\mathbb{Z}$ is a ring, we have

$$\begin{aligned}
[(\alpha \cdot \beta) \cdot \gamma](g) &= [\phi \cdot \gamma](g) \\
&= \sum_{\substack{f,c \in G \\ fc=g}} \phi(f)\gamma(c) \\
&= \sum_{\substack{a,b,c \in G \\ abc=g}} \alpha(a)\beta(b)\gamma(c) \\
&= \sum_{\substack{a,h \in G \\ ah=g}} \alpha(a)\psi(h) \\
&= [\alpha \cdot \psi](g) \\
&= [\alpha \cdot (\beta \cdot \gamma)](g).
\end{aligned}$$

It remains to see that the distributive laws hold. We only show that $(\phi + \psi)\gamma = \phi\gamma + \psi\gamma$. The other distributive law is proved similarly. We use the fact that $\mathbb{Z}$ is a ring. We have

$$\begin{aligned}
[(\phi + \psi)\gamma](g) &= \sum_{\substack{f,h \in G \\ fh=g}} [\phi + \psi](f)\gamma(h) \\
&= \sum_{\substack{f,h \in G \\ fh=g}} (\phi(f)\gamma(h) + \psi(f)\gamma(h)) \\
&= \sum_{\substack{f,h \in G \\ fh=g}} \phi(f) \cdot \gamma(h) + \sum_{\substack{f,h \in G \\ fh=g}} \psi(f) \cdot \gamma(h) \\
&= [\phi \cdot \gamma](g) + [\psi \cdot \gamma](g).
\end{aligned}$$