Problem sheet 7

1. (a) The sum of two elements of this form is still of this form: $(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$ with $a + c, b + d \in \mathbb{Q}$. The sum is asosciative (it is the usual sum in $\mathbb{R}$), the identity element if 0, and the inverse of $a + b\sqrt{2}$ is $-a - b\sqrt{2}$ (since their sum is 0, the identity element). Therefore this set, with operation the sum, is a group.

   It is not a group with operation the product: The identity element would have to be 1 (you want the identity e to have the property $e \cdot (a + b\sqrt{2}) = a + b\sqrt{2}$), but in this case the element 0 would have no inverse (you cannot multiply zero by something and get 1).

   (b) With the sum: For the identity e, to obtain $e + A = A$ for every A, we must have e to be the zero matrix. But the zero matrix is not invertible, so does not belong to our set. It is not a group.

   With the product: The product of 2 invertible matrices is invertible, the product of matrices is associative. For the identity, we want a matrix e such that $e \cdot A = A \cdot e = A$. We take the identity matrix (we can, it is invertible, so it is in our set). For the inverse, we take the usual inverse of matrices (the result is an invertible matrix, it belongs to the set we consider). So it is a group.

2. Consider the row correspoding to the element a. It contains all the elements of the form ab for $b \in G$ (and such a result appears only once for each element b). If $c \in G$, then $c = a(a^{-1}c)$, so c appears in the row. If c were to appear twice, it would mean $c = ae = af$ for some $e \neq f$. But $ae = af$ implies $e = f$, so it is not possible.

3. The first row tells us $ac = a$, so $c = e$ the identity element. It allows us to fill the column under c and the row right of c. Now the row right of b contains every group element except c, so we know by the previous exercise that we need to put c in the empty slot. It gives us $ba = c$. Since c is the identity, it means that b is the inverse of a (and a the inverse of b), so $ab = c$, we can put that in the table. The second row gives us $bd = a$, therefore $abd = a^2$ and thus $d = a^2$ (since a is the inverse of b), we can put this in the table. Now ompleting the rest is easy using the previous exercise.

   The group is Abelian because it is symmetric across the diagonal (since Abelian means that we have $xy = yx$ for every x, y).

   There are probably plenty of different ways to proceed to fill in this table.

4. We have

$$a^2 = a_1 a_2 \cdots a_n \cdot a_1 a_2 \cdots a_n.$$

The idea is that the inverse of each a_i from the "first part" of this product is in G, so is some a_j which appears in the "second part" of the product. We can regroup them all since G is Abelian, they all cancel out and we get e.

The difficulty is to write it somewhat clearly. Here is one way to do it, it consists in giving a name $a_{f(i)}$ to the inverse of a_i, so that we can "talk" about it more easily. I am sure there are other, possibly better, ways to present this.

For a_i in G, let $a_{f(i)}$ be the inverse of a. This defines a map $f : \{1, \ldots, n\} \to \{1, \ldots, n\}$. This map is injective (if $f(i) = f(j)$ then $a_i^{-1} = a_j^{-1}$, so $a_i = a_j$ and thus $i = j$). Why observe this? Because since f goes from $\{1, \ldots, n\}$ to $\{1, \ldots, n\}$ is implies that f is surjective, so $\{a_{f(1)}, \ldots, a_{f(n)}\} = \{a_1, \ldots, a_n\}$. It gives us a way to pair each element with its inverse in the product a^2 (using that G is Abelian, so we can change the order of elements in a product):

$$\begin{aligned} a^2 &= a_1 a_2 \cdots a_n \cdot a_{f(1)} a_{f(2)} \cdot a_{f(n)} \\ &= a_1 a_{f(1)} a_2 a_{f(2)} \cdots a_n a_{f(n)} \\ &= ee \cdots e \\ &= e. \end{aligned}$$