MTHM024/MTH714U **Group Theory**

Problem Sheet 4 **Solutions**

---

1 (a) If $n=2$, then Ω contains only the single element $\{1,2\}$, and obviously every element of S_2 fixes it; so the action is not faithful. (If $g=(1,2)$, then $\{1,2\}g = \{1g,2g\} = \{2,1\} = \{1,2\}$.)

(b) If $n=3$, the map

$$\{1,2\} \mapsto 3, \qquad \{2,3\} \mapsto 1, \qquad \{1,3\} \mapsto 2$$

is an isomorphism from the action on Ω to the usual action on $\{1,2,3\}$, which is obviously doubly transitive.

(c) If $n=4$, then the relation $\{i,j\} \sim \{k,l\}$ if the sets $\{i,j\}$ and $\{k,l\}$ are equal or disjoint, is a congruence: it is obviously invariant under S_4, and the fact that it is an equivalence relation is most easily seen by observing that the three equivalence classes form a partition of Ω. So S_4 is imprimitive.

(d) Assume that $n \geq 5$. To show that the action of S_n on Ω is primitive, suppose that $\equiv$ is a congruence, which is not the relation of equality, so two unequal pairs are congruent. There are two cases:

- Two pairs with an element in common, say $\{a,b\}$ and $\{a,c\}$, are congruent. Since S_n acts transitively on configurations like this, it follows that every two pairs with an element in common are congruent. Then for example, $\{1,2\}$ is congruent to $\{1,3\}$ and to $\{2,4\}$; so two disjoint pairs are also congruent. Now reason as in the next case.

- Two disjoint pairs are congruent, say $\{a,b\}$ and $\{c,d\}$. Again S_n is transitive on such configurations, so every two disjoint pairs are congruent. Now $\{1,2\}$ is congruent to $\{3,4\}$ and to $\{3,5\}$ [here we use the fact that $n \geq 5$], so two pairs with an element in common are congruent. Now reason as in the preceding case.

The conclusion is that any two pairs are congruent, so the congruence is the universal relation. Thus the group is primitive.

To show it is not doubly transitive, observe that a permutation cannot map two intersecting pairs like $\{1,2\}$ and $\{1,3\}$ to two disjoint pairs like $\{1,2\}$ and $\{3,4\}$.

2 (a) Any automorphism of a group G must permute the elements of G and fix the identity, so must permute the non-identity elements. If $G = V_4$, there are three non-identity elements, so $\mathrm{Aut}(G) \leq S_3$. Why is it equal to S_3? One way to see this is to observe that, if $V_4 = \{1, a, b, c\}$, then we can specify the multiplication as follows:

- $1x = x1 = x$ and $x^2 = 1$ for all $x \in G$;
- the product of any two distinct non-identity elements is the third.

Stated in this way, it is clear that any permutation of the non-identity elements is an automorphism of the group.

(b) Let $G = S_3$. Since $Z(G) = \{1\}$, we have

$$G \cong \mathrm{Inn}(G) \leq \mathrm{Aut}(G),$$

and we are done if we can show that G has at most six automorphisms. But G has two elements of order 3 and three of order 2; any choice of an element a of order 3 and b of order 2 generates the group, so an automorphism is uniquely determined by what it does to a and b. And a must go to an element of order 3, and b to an element of order 2, so there are at most $2 \cdot 3 = 6$ choices.

(c) For $n > 2$ and $n \neq 6$, the symmetric group has trivial centre and no outer automorphisms; so

$$\mathrm{Aut}(S_n) \cong \mathrm{Inn}(S_n) \cong S_n / Z(S_n) \cong S_n.$$

Many other examples are possible, for example dihedral groups of order greater than 4.

(d) Suppose that G is elementary abelian of order 8. Then G is isomorphic to the additive group of a 3-dimensional vector space over the field $\mathbb{Z}_2$ with two elements. Any map taking a basis to a basis extends uniquely to an automorphism. So the order of the automorphism group is equal to the number of bases. Now there are

- 7 choices for the first basis vector u (any non-zero vector);
- 6 choices for the second basis vector v (any vector which is not a multiple of u, thus 0 and u are excluded);
- 4 choices for the third basis vector (any vector which is not a linear combination of u and v, thus 0, u, v and $u + v$ are excluded).

Now it is a simple exercise to label the Fano plane with the seven non-zero vectors of the 3-dimensional vector space in such a way that three points form a line if and only if the corresponding vectors sum to 0. So any automorphism of the group will be an automorphism of the Fano plane. Since the two automorphism groups have the same order 168, they are equal.

3 If G is non-abelian, suppose that $gh \neq hg$. Then conjugation by g (the map $x \mapsto g^{-1}xg$) is an (inner) automorphism of G, and is not the identity, since it doesn't fix h.

If G is abelian, then the map $\mapsto x^{-1}$ is an automorphism, since $(xy^) - 1 = y^{-1}x^{-1} = x^{-1}y^{-1}$. If some element of G is not equal to its inverse, then this automorphism is non-trivial. [Note that the map $x \mapsto x^{-1}$ is an automorphism of G if and only if G is abelian.]

Finally, if every element of G is equal to its inverse, then G is an elementary abelian 2-group, and so is isomorphic to the additive group of a k-dimensional vector space over $\mathbb{Z}_2$ (where $|G| = 2^k$). Since $|G| > 2$ we have $k > 1$. Now choose a basis for G; the map which switches the first two basis vectors and fixes the rest is a non-trivial automorphism.

All of this works exactly the same for infinite groups except for the innocent-looking phrase "choose a basis". The proof that every (infinite-dimensional) vector space has a basis requires the Axiom of Choice.