Group Theory: Math30038, Sheet 7

Solutions – GCS

1. *Suppose that $n \geq 3$. Let $g \in G = S_n$ be an n-cycle. Recall that all n-cycles are conjugate in S_n.*

   (a) *Prove that $C_G(g) = \langle g \rangle$.*
   Solution Since the conjugacy class of g has size $(n-1)!$ it follows that $C_G(g)$ has order n and so is $\langle g \rangle$.

   (b) *Deduce that $Z(G) = 1$.*
   Solution Let $g_1 = (1, 2, 3, \dots, n)$ and $g_2 = (2, 1, 3, \dots n)$ (so g_1 and g_2 only differ in their effects on 1 and 2). Now $Z(G) \leq C_G(g_1) \cap C_G(g_2) = \langle g_1 \rangle \cap \langle g_2 \rangle = 1$.

   (c) *Show that $Aut(G)$ has a subgroup which is isomorphic to G.*
   Solution Let $\tau : G \longrightarrow \mathrm{Aut}(G)$ be the homomorphism which sends each group element x to the automorphism τ_x which is "conjugation by x". Now $\mathrm{Ker}\ \tau = Z(G) = 1$ so τ is a monomorphism and $\mathrm{Im}\ \tau$ is a subgroup of $\mathrm{Aut}(G)$ which is isomorphic to G as required.

2. *Suppose that G is a group and that $Aut(G)$ is the trivial group.*

   (a) *Show that G must be abelian.*
   Solution If $x \in G - Z(G)$, then τ_x (conjugation by x) will be a non-trivial automorphism of G. Thus $G - Z(G) = \emptyset$ so $G = Z(G)$ is abelian.

   (b) *By considering the inversion map, deduce that $g^2 = 1$ for all $g \in G$.*
   Solution The inversion map is a non-trivial automorphism unless $g = g^{-1}$ for every $g \in G$, so $g^2 = 1$ for all $g \in G$.

(c) *Write G additively, so that G becomes a vector space over the field $\mathbb{Z}_2$ of "integers modulo 2". You may assume that every vector space has a basis. Deduce that G must either be cyclic of order 2 or the trivial group.*

Solution Pick a basis B of the vector space G. If dim $G > 1$, then we can choose two distinct elements u, v of B. Now the map which swaps u and v and fixes all other elements of B extends uniquely to a non-trivial linear isomorphism from G to G. This linear isomorphism will also be a non-trivial group automorphism of G. We deduce that G has dimension 0 or 1, and so is either the trivial group or the cyclic group of order 2. Finally we observe that these two groups do indeed have trivial groups of automorphisms.

3. *Suppose that G is a group and that $Aut(G)$ is finite. Prove that $|G : Z(G)|$ must be finite.*

   Solution $G/Z(G)$ is isomorphic to a subgroup of Aut G, and so is finite. Thus $|G : Z(G)|$ is finite.

4. *(Challenge) Suppose that G is a group and that $Aut(G)$ is cyclic. Prove that G must be abelian.*

   Solution Since a subgroup of a cyclic group is cyclic, it follows that $G/Z(G)$ is a cyclic group. Say $G/Z(G)$ is generated by $tZ(G)$. Thus every element of G lies in a coset $t^k Z(G)$ for some integer k, and therefore $G = \langle \{t\} \cup Z(G) \rangle$. Thus G is abelian.

5. *Prove that for a finite group, the notions of isomorphism, monomorphism and epimorphism all co-incide.*

   Solution This was poorly worded. I was thinking of homomorphisms from a finite group G to itself (so called endomorphism of G). Since G is finite, the notions of injection, surjection and bijection all co-incide.

6. In each case give an example of a group G and a map $\zeta : G \to G$ which satisfies the specified property.

   (a) *An epimorphism (i.e. a surjective homomorphism) but not an isomorphism (suggestion for G: fix a prime number p and consider those complex numbers z such that $z^{p^n} = 1$ for some natural number n which may vary as z varies).*

   Solution The map whic sends each element to its p-th power is a homomorphism, and is surjective but not injective.

(b) *A monomorphism (i.e. an injective homomorphism) but not an isomorphism (suggestion for G: $\mathbb{Z}$ under addition).*
Solution The map which doubles every integer is an injective homomorphism, but is clearly not surjective.

7. *Suppose that G is a finitely generated group (i.e. there is a finite subset X of G such that $\langle X \rangle = G$) and that every conjugacy class of G is finite. Prove that $|G : Z(G)|$ is finite.*
Solution Since every conjugacy class is finite, each centralizer of an element is of finite index in G. Now an element is in the centre of G if and only if it commutes with every element of a generating set. Thus

$$Z(G) = \cap_{x \in X} C_G(x).$$

Now, we have proved that the intersection of two (and therefore finitely many) subgroups of finite index is of finite index. Since X is finite it follows that $|G : Z(G)| < \infty$.

8. *Let V be a vector space of dimension n over a field F which has q elements. Let $GL(V)$ denote the group of linear isomorphisms from V to V (a group under composition of maps). Determine $|GL(V)|$.*
Solution Pick and fix a basis for use both in domain and codomain. The invertible linear maps on V are in bijective correspondence with the invertible n by n matrices. we count such matrices row by row. The first row (viewed as an element of F^n) can be any non-zero vector, of which there are $q^n - 1$. The second row must not be a linear multiple of the first, yielding $q^n - q$ choices. The first two rows are now linearly independent, and their span must have size q^2. The third row can be any vector not in the span of the first two rows, giving us $q^n - q^2$ possibilities.

Continuing in this fashion, we deduce that

$$|GL(V)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

9. (a) *Suppose that G is a group acting on a set Ω. Define a map $\eta : G \longrightarrow Sym(\Omega)$ by $(g)\eta : \omega \mapsto \omega \cdot g$ for all $\omega \in \Omega$ and for all $g \in G$. Prove that η is a homomorphism of groups.*
Solution Suppose that $u, v \in G$, then $(uv)\eta : \omega \mapsto \omega \cdot (uv) = (\omega \cdot u) \cdot v$. On the other hand $(u)\eta \circ (v)\eta : \omega \mapsto (\omega \cdot u) \cdot v$.

Now for each $g \in G$ we have $(g)\eta \circ (g^{-1})\eta = (g^{-1})\eta \circ (g)\eta = (1)\eta$ which is the identity map. Therefore each $(g)\eta$ has a two-sided inverse and so is an element of $\mathrm{Sym}(\Omega)$. We have already established the multiplicativity property which ensures that η is a group homomorphism.

(b) *Suppose that $\eta : G \longrightarrow Sym(\Omega)$ is a group homomorphism. Show that one may define a group action of G on the set Ω by defining $\omega \cdot g$ to be $(\omega)((g)\eta)$ for all $\omega \in \Omega$ and for all $g \in G$. Show that this is indeed a group action.*

Solution Now suppose that $\eta : G \to \mathrm{Sym}(\Omega)$ is a group homomorphism. We define an action of G on Ω by $\omega \cdot g = (\omega)(g)\eta$. We check that this is an action: $\omega \cdot 1 = (\omega)(1)\eta = (\omega)\mathrm{Id}_\Omega = \omega$ for every $\omega \in \Omega$. Also if $u, v \in G$, then $\omega \cdot (uv) = (\omega)(uv)\eta = (\omega)((u)\eta(v)\eta) = ((\omega)(u)(\eta))(v)(\eta) = (\omega \cdot u) \cdot v$. Thus we have an action.

(c) *Show that the procedures outlined in parts (a) and (b) are mutually inverse (i.e. if you perform one, then the other, then you recover the situation in which you started).*

Solution Suppose that we have an action denoted by a dot which gives rise to the group homomorphism $\eta : G \to \mathrm{Sym}(\Omega)$ outlined in part (a). Now we use part (b) to define an action of G on Ω denoted $\star$. The definition of $\star$ is that if $\omega \in \Omega$ and $g \in G$, then $\omega \star g = (\omega)((g)\eta) = \omega \cdot g$. Thus $\star$ is the same action as the original one. Conversely suppose that you have a homomorphism $\eta : G \to \mathrm{Sym}(\Omega)$. This gives rise to an action as outlined in part (b). According to part (a) this gives rise to a homomorphism $\xi : G \to \mathrm{Sym}(\Omega)$ defined by $(g)\xi : \omega \mapsto \omega \cdot g = (\omega)(g)\eta$. Thus the maps $(g)\xi$ and $(g)\eta$ have the same domains and codomains, and agree at all arguments. Thus $(g)\xi = (g)\eta$ for every g, and so $\xi = \eta$.