# MAU22101: Solutions Week 5

**Problem 1** Let $G \times X \to X$ be a transitive $G$-action and let $x \in X$. Show that there is an isomorphism of $G$-sets

$$\begin{aligned} \phi\colon G/\mathrm{Stab}_G(x) &\to X \\ [g] &\mapsto g.x, \end{aligned}$$

where $\mathrm{Stab}_G(x) := \{g \in G \mid g.x = x\}$ is the stabilizer subgroup of $G$. That is, show that

i) $\phi$ is well-defined,

ii) $\phi$ is a homomorphism of $G$-sets,

iii) $\phi$ is a bijection.

**Solution 1**

*i) We verify that whenever $[g_1] = [g_2]$ then also $g_1.x = g_2.x$. But $[g_1] = [g_2]$ implies that $g_2^{-1}g_1 \in \mathrm{Stab}_G(X)$ and thus*

$$g_1.x = (g_2g_2^{-1}g_1).x = g_2.((g_2^{-1}g_1).x) = g_2.x,$$

*where we used that $g_2^{-1}g_1.x = x$ in the last equation.*

*ii) Recall that the set of left cosets $G/H$ is a $G$-set via the action $h.[g] = h.(gH) = hgH = [hg]$. We thus compute*

$$\phi(h.[g]) = \phi([hg]) = (hg).x = h.(g.x) = h.\phi([g]).$$

*iii) Since the action is assumed to be transitive, i.e. there is exactly one orbit, we conclude that $G.x = X$. But this is exactly surjectivity for $\phi$. Namely, it says that for every $y \in X$ there exists $g \in G$ such that $y = g.x = \phi([g])$ showing that $\phi$ is surjective. For injectivity, suppose we have $[g_1], [g_2] \in G/\mathrm{Stab}_G(X)$ such that*

$$\phi([g_1]) = \phi([g_2]),$$

*which we write out as*

$$g_1.x = g_2.x.$$

*From this we get that*

$$(g_2^{-1}g_1).x = g_2^{-1}.(g_1.x) = g_2^{-1}.(g_2.x) = (g_2^{-1}.g_2).x = x,$$

*which implies that $g_2^{-1}g_1 \in \mathrm{Stab}_G(X)$ and thus $[g_1] = [g_2]$.*

**Problem 2** Let $G \times X \to X$ be a $G$-action and let $V \subset X$ be a $G$-orbit. Given $x, y \in V$ show that there exists $g \in G$ such that

$$\mathrm{Stab}_G(x) = g\mathrm{Stab}_G(y)g^{-1}$$

(i.e. the corresponding stabilizer subgroups are conjugate).

**Solution 2** *Since $x$ and $y$ lie in the same orbit (and distinct orbits are disjoint) we obtain that $G.x = V = G.y$. In particular, we obtain that $x \in G.y$ and thus there exists $g \in G$ such that $x = g.y$ (and hence also $y = g^{-1}.x$). We now show that*

$$\mathrm{Stab}_G(x) = g\mathrm{Stab}_G(y)g^{-1}$$

*for our choice of $g$ by showing the two inclusions. Let $ghg^{-1} \in g\mathrm{Stab}_G(Y)g^{-1}$ (that is, $h \in \mathrm{Stab}_G(y)$), then*

$$ghg^{-1}.x = gh.y = g.y = x$$

*and thus $ghg^{-1} \in \mathrm{Stab}_G(x)$. For the other inclusion, let $h \in \mathrm{Stab}_G(x)$ and compute*

$$g^{-1}hg.y = g^{-1}h.x = g^{-1}x = y,$$

*which implies that $g^{-1}hg \in \mathrm{Stab}_G(y)$ and thus $h = g(g^{-1}hg)g^{-1} \in g\mathrm{Stab}_G(y)g^{-1}$.*

**Problem 3** Let $N \lhd G$ be a normal subgroup and let $\pi \colon G \to G/N$ be the canonical projection map $\pi(x) = [x]$. Show that there is a one-to-one correspondence

$$\begin{aligned} \{\text{subgroups of } G/N\} &\longleftrightarrow \{\text{subgroups of } G \text{ containing } N\} \\ H &\mapsto \pi^{-1}(H) \\ K/N &\leftarrow K. \end{aligned}$$

Moreover, show that $\pi^{-1}(K/N) = KN$ for any subgroup $K \leqslant G$ (not necessarily containing $N$).

**Solution 3** *Let us first give names to the two assignments. Let $\mathcal{F}(H) := \pi^{-1}(H)$ and $\mathcal{G}(K) := K/N$.*

- **$\mathcal{F}$ is well-defined:** *We first check that $\pi^{-1}(H)$ is indeed a group. Given $x, y \in \pi^{-1}(H)$ we have that $\pi(xy^{-1}) = \pi(x)\pi(y)^{-1} \in H$ hence $xy^{-1} \in \pi^{-1}(H)$, showing that $\pi^{-1}(H)$ is indeed a subgroup of $G$. Moreover, since $\{e\} \in H$ we have*

  $$N = \ker(\pi) = \pi^{-1}(\{e\}) \subset \pi^{-1}(H).$$

- **$\mathcal{G} \circ \mathcal{F} = \mathrm{id}$:** *We first note that $\mathcal{G}(K) = \pi(K)$. Since $\pi$ is surjective we obtain that*

  $$\mathcal{G}(\mathcal{F}(H)) = \pi(\pi^{-1}(H)) = \pi(\pi^{-1}(H)) = H$$

  *holds for any subset $H \subset G$, in particular for subgroups.*

- **$\mathcal{F} \circ \mathcal{G} = \mathrm{id}$:** *Let $K \leqslant G$ be a subgroup. Then $x \in \mathcal{F}(\mathcal{G}(K))$ if and only if*

  $$\begin{aligned} \pi(x) \in \mathcal{G}(K)) &\iff [x] \in K/N \\ &\iff xN = kN \text{ for some } h \in K \\ &\iff k^{-1}x \in N \text{ for some } k \in K \\ &\iff x = kn \text{ for some } k \in K \text{ and } n \in N \\ &\iff x \in KN \end{aligned}$$

  *This shows the "moreover" part of the problem. If $K$ already contains $N$ then we have $KN = N$ and thus $\mathcal{F}(\mathcal{G}(K)) = K$.*

**Problem 4** Prove that the additive group of rational numbers $(\mathbb{Q}, +)$ has no proper subgroups of finite index.

**Solution 4** *Let $H \leqslant \mathbb{Q}$ be a finite-index subgroup of $\mathbb{Q}$. Since $\mathbb{Q}$ is abelian, we obtain that the quotient is a group $\mathbb{Q}/H$, which is assumed to be finite. In particular, by a consequence of Lagrange's theorem, we have $[x]^n = e$ for $n = |\mathbb{Q}/H|$. This means that for any $q \in \mathbb{Q}$ we have that $nq \in H$ (recall that the group operation is addition). But this implies that $H = \mathbb{Q}$ as*

$$q = n(q/n) \in H.$$

**Problem 5** Prove Fermat's little theorem that for $a \in \mathbb{Z}$ and a prime $p$ we have

$$a^p \equiv a \pmod{p}.$$

(Hint: use Lagrange's theorem in the group $(\mathbb{Z}/p\mathbb{Z})^\times$.)

**Solution 5** *Recall that the group $(\mathbb{Z}/p\mathbb{Z})^\times$ contains an element $\bar{k} \in \mathbb{Z}/p\mathbb{Z}$ if and only if $(k, p) = 1$. Since $p$ is prime, this means that*

$$(\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}.$$

*That is, the only element that is excluded is $\bar{0}$, and so we get*

$$|(\mathbb{Z}/p\mathbb{Z})^\times| = p - 1.$$

*By Lagrange's theorem we have that*

$$a^{p-1} = \bar{1},$$

*for all $p \in (\mathbb{Z}/p\mathbb{Z})^\times$. Or in other words, we have*

$$a^{p-1} \equiv 1 (mod\ p),$$

*for all $a \in \mathbb{Z}$ such that $(a, p) = 1$. But then we also have*

$$a^p \equiv a(mod\ p),$$

*for the same $a$'s. In the case $(a, p) \neq 1$ we have that $p \mid a$ but then the equation is also true.*