G.6. Proofs: Group actions

Proposition G.6.1. — *Suppose G is a group acting on a set S and let $s \in S$ and $g \in G$. Then*
(a) *G_s is a subgroup of G.*
(b) *$G_{gs} = gG_sg^{-1}$.*

Proof. —
(a) To show: (aa) If $h_1, h_2 \in G_s$ then $h_1h_2 \in G_s$.
(ab) $1 \in G_s$.
(ac) If $h \in G_s$ then $h^{-1} \in G_s$.

(aa) Assume $h_1, h_2 \in G_s$.
Then
$$(h_1h_2)s = h_1(h_2s) = h_1s = s.$$
So $h_1h_2 \in G_s$.
(ab) Since $1s = s, 1 \in G_s$.
(ac) Assume $h \in G_s$.
Then
$$h^{-1}s = h^{-1}(hs) = (h^{-1}h)s = 1s = s.$$
So $h^{-1} \in G_s$.

So G_s is a subgroup of G.
(b) To show: (ba) $G_{gs} \subseteq gG_sg^{-1}$.

(bb) $gG_sg^{-1} \subseteq G_{gs}$.

(ba) Assume $h \in G_{gs}$.
Then $hgs = gs$.
So $g^{-1}hgs = s$.
So $g^{-1}hg \in G_s$.
Since $h = g(g^{-1}hg)g^{-1}$ then $h \in gG_sg^{-1}$.
So $G_{gs} \subseteq gG_sg^{-1}$.
(bb) Assume $h \in gG_sg^{-1}$.
So there exists $a \in G_s$ such that $h = gag^{-1}$.
Then
$$hgs = (gag^{-1})gs = gas = gs.$$
So $h \in G_{gs}$.
So $G_{gs} \subseteq gG_sg^{-1}$.

So $G_{gs} = gG_sg^{-1}$. □

Proposition G.6.2. — *Let G be a group which acts on a set S. Then the orbits partition the set S.*

Proof. —
To show: (a) If $s \in S$ then there exists $t \in S$ such that $s \in Gt$.
(b) If $s_1, s_2 \in S$ and $Gs_1 \cap Gs_2 \neq \emptyset$ then $Gs_1 = Gs_2$.

(a) Assume $s \in S$.
Then, since $s = 1s, s \in Gs$.
(b) Assume $s_1, s_2 \in S$ and that $Gs_1 \cap Gs_2 \neq \emptyset$.

Let $t \in Gs_1 \cap Gs_2$.
Then there exist $g_1, g_2 \in G$ such that $t = g_1s_1$ and $t = g_2s_2$.
So

$$s_1 = g_1^{-1}g_2s_2 \text{ and } s_2 = g_2^{-1}g_1s_1.$$

To show: $Gs_1 = Gs_2$.
To show: (ba) $Gs_1 \subseteq Gs_2$.
(bb) $Gs_2 \subseteq Gs_1$.

(ba) Let $t_1 \in Gs_1$.
So there exists $h_1 \in G$ such that $t = h_1s_1$.
Then

$$t_1 = h_1s_1 = h_1g_1^{-1}g_2s_2 \in Gs_2.$$

So $Gs_1 \subseteq Gs_2$.

(bb) Let $t_2 \in Gs_s$.
So there exists $h_2 \in G$ such that $t_2 = h_2s_2$.
Then

$$t_2 = h_2s_2 = h_2g_2^{-1}g_1s_1 \in Gs_1.$$

So $Gs_2 \subseteq Gs_1$.

So $Gs_1 = Gs_2$.

So the orbits partition S. □

Corollary G.6.3. — *If G is a group acting on a set S and Gs_i denote the orbits of the action of G on S then*

$$\mathrm{Card}(S) = \sum_{\text{distinct orbits}} \mathrm{Card}(Gs_i).$$

Proof. — By Proposition 1.2.4, S is a disjoint union of orbits.
So Card(S) is the sum of the cardinalities of the orbits. □

Proposition G.6.4. — *Let G be a group acting on a set S and let $s \in S$. If Gs is the orbit containing s and G_s is the stabilizer of s then*

$$\mathrm{Card}(G/G_s) = \mathrm{Card}(Gs).$$

where G/G_s is the set of cosets of G_s in G.

Proof. — To show: There is a bijective map $\varphi\colon\ G/G_s \to Gs$.
Define

$$\begin{array}{rccc} \varphi\colon & G/G_s & \to & Gs \\ & gG_s & \mapsto & gs. \end{array}$$

To show: (a) φ is well defined. (b) φ is bijective.

(a) To show: (aa) If $g \in G$ then $\varphi(gG_s) \in Gs$.
(ab) If $g_1G_s = g_2G_s$ then $\varphi(g_1G_s) = \varphi(g_2G_s)$.

(aa) From the definition of φ, $\varphi(gG_s) = gs \in Gs$.

(ab) Assume $g_1, g_2 \in G$ and $g_1G_s = g_2G_s$.
Then $g_1 = g_2h$ for some $h \in G_s$.
To show: $g_1s = g_2s$.
Since $h \in G_s$ then $g_1s = g_2hs = g_2s$.
So $\varphi(g_1G_s) = \varphi(g_2G_s)$.

So φ is well defined.

(b) To show: (ba) φ is injective.
(bb) φ is surjective.

(ba) To show: φ is injective.
If $\varphi(g_1G_s) = \varphi(g_2G_2)$ then $g_1G_s = g_2G_s$.
Assume $\varphi(g_1G_s) = \varphi(g_2G_s)$.
Then $g_1s = g_2s$.
So $s = g_1^{-1}g_2s$ and $g_2^{-1}g_1s = s$.
So $g_1^{-1}g_2 \in G_s$ and $g_2^{-1}g_1 \in G_s$.
To show: $g_1G_s = g_2G_s$
To show: (baa) $g_1G_s \subseteq g_2G_s$.
(bab) $g_2G_s \subseteq g_1G_s$.

(baa) Let $k_1 \in g_1G_s$.
So there exists $h_1 \in G_s$ such that $k_1 = g_1h_1$.
Then

$$k_1 = g_1h_1 = g_1g_1^{-1}g_2g_2^{-1}g_1h_1 = g_2(g_2^{-1}g_1h_1) \in g_2G_s.$$

So $g_1G_s \subseteq g_2G_s$.

(bab) Let $k_2 \in g_2G_s$.
So there exists $h_2 \in G_s$ such that $k_2 = g_2h_2$.
Then

$$k_2 = g_2h_2 = g_2g_2^{-1}g_1g_1^{-1}g_2h_2 = g_1(g_1^{-1}g_2h_2) \in g_1G_s.$$

So $g_2G_s \subseteq g_1G_s$.
So $g_1G_s = g_2G_s$.
So φ is injective.

(bb) To show: φ is surjective.
To show: If $t \in Gs$ then there exists $hG_s \in G/G_s$ such that $\varphi(hG_s) = t$.
Assume $t \in G_s$.
Then there exists $g \in G$ such that $t = gs$.
Let $h = g$ so that $hG_s = gG_s$.
Then $\varphi(gG_s) = gs = t$.
So φ is surjective.

So φ is bijective. □

Corollary G.6.5. — *Let G be a group acting on a set S. Let $s \in S$, let G_s denote the stabilizer of s and let Gs denote the orbit of s. Then*

$$\mathrm{Card}(G) = \mathrm{Card}(Gs)\mathrm{Card}(G_s).$$

Proof. — Multiply both sides of the identity in Proposition 1.2.6 by $\mathrm{Card}(G_s)$ and use Corollary 1.1.5. □

Proposition G.6.6. — *Let H be a subgroup of G and let N_H be the normalizer of H in G. Then*
(a) *H is a normal subgroup of N_H.*
(b) *If K is a subgroup of G such that $H \subseteq K \subseteq G$ and H is a normal subgroup of K then $K \subseteq N_H$.*

Proof. —
(b) Assume K is a subgroup of G, $H \subseteq K \subseteq G$ and H is a normal subgroup of K.
To show: $K \subseteq N_H$.

Let $k \in K$.
To show: $k \in N_H$.
To show: If $h \in H$ then $khk^{-1} \in H$.
This is true since H is normal in K.
So $K \subseteq N_H$.

(a) This is the special case of (b) when $K = H$. □

Proposition G.6.7. — *Let G be a group and let $\mathcal{S}$ be the set of subsets of G. Then*
(a) *G acts on $\mathcal{S}$ by*

$$\begin{array}{rccc} \alpha\colon & G \times \mathcal{S} & \to & \mathcal{S} \\ & (g, S) & \mapsto & gSg^{-1} \end{array} \qquad \textit{where } gSg^{-1} = \{gsg^{-1} \mid s \in S\}.$$

We say that G acts on $\mathcal{S}$ by conjugation.
(b) *If S is a subset of G then N_S is the stabilizer of S under the action of G on $\mathcal{S}$ by conjugation.*

Proof. —
(a) To show: (aa) α is well defined.
(ab) $\alpha(1, S) = S$ for all $S \in \mathcal{S}$.
(ac) If $g, h \in G$ and $S \in \mathcal{S}$ then $\alpha(g, \alpha(h, S)) = \alpha(gh, S)$.
(aa) To show: (aaa) $gSg^{-1} \in \mathcal{S}$.
(aab) If $S = T$ and $g = h$ then $gSg^{-1} = hTh^{-1}$.
Both of these are consequences of the definitions.
(ab) Let $S \in \mathcal{S}$.
Then $\alpha(1, S) = 1S1^{-1} = S$.
(ac) Let $g, h \in G$ and $S \in \mathcal{S}$.
Then

$$\alpha\big(g, \alpha(h, S)\big) = \alpha(g, hSh^{-1}) = g(hSh^{-1})g^{-1} = (gh)S(h^{-1}g^{-1}) = (gh)S(gh)^{-1} = \alpha(gh, S).$$

(b) This follows from the definitions of N_S and of stabilizer. □

Proposition G.6.8. — *Let G be a group. Then*
(a) *G acts on G by*

$$\begin{array}{ccc} G \times G & \to & G \\ (g, s) & \mapsto & gsg^{-1}. \end{array}$$

We say that G acts on itself by conjugation.
(b) *Two elements $g_1, g_2 \in G$ are conjugate if and only if they are in the same orbit under the action of G on itself by conjugation.*
(c) *Let $g \in G$. The conjugacy class $\mathcal{C}_g$ is the orbit of g under the action of G on itself by conjugation.*
(d) *Let $g \in G$. The centralizer Z_g is the stabilizer of g under the action of G on itself by conjugation.*

Proof. —
(a) The proof is exactly the same as the proof of (a) in Proposition 1.2.10.
Replace all the capital S's by lower case s's.
(b), (c), and (d) follow from the definitons. NOT SURE IF I LIKE THIS. □

Lemma G.6.9. — *Let G_s be the stabilizer of $s \in G$ under the action of G on itself by conjugation. Let $Z(G)$ be the center of G. Let S be a subset of G. Then*

(a) $Z_S = \bigcap_{s\in S} G_s$.
(b) $Z(G) = Z_G$.
(c) $s \in Z(G)$ *if and only if* $Z_s = G$.
(d) $s \in Z(G)$ *if and only if* $\mathcal{C}_s = \{s\}$.

Proof. —
(a)
(aa) Assume $s \in Z_s$.
Then, if $\in S$ then $sxs^{-1} = s$.
So, if $s \in S$ then $x \in G_s$.
So $x \in \bigcap_{s\in S} G_s$.
So $Z_s \subseteq \bigcap_{s\in S} G_s$.
(ab) Assume $x \in \bigcap_{s\in S} G_s$.
Thus, if $s \in S$ then $xsx^{-1} = s$.
So $x \in Z_s$.
So $\bigcap_{s\in S} G_s \subseteq Z_s$.
(b) This follows from the definitions of Z_G and $Z(G)$.
(c) $\Longrightarrow$:
Let $s \in Z(G)$.
To show: $Z_s = G$.
By definition, $Z_s \subseteq G$.
To show: $G \subseteq Z_s$.
Let $g \in G$.
Then $gsg^{-1} = s$, since $s \in Z(G)$.
So $g \in Z_s$.
So $G \subseteq Z_s$.
So $Z_s = G$.

(c) $\Longleftarrow$:
Assume $Z_s = G$.
So, if $g \in G$ then $gsg^{-1} = s$.
Thus, if $g \in G$ then $gs = sg$.
So $s \in Z(G)$.

(d) $\Longrightarrow$:
Assume $s \in Z(G)$.
Then, if $s \in G$ then $gsg^{-1} = s$.
So $\mathcal{C}_s = \{gsg^{-1} \mid g \in G\} = \{s\}$.

(d) $\Longleftarrow$:
Assume $\mathcal{C}_s = \{s\}$.
So, if $g \in G$ then $gsg^{-1} = s$.
So $s \in Z(G)$.

□

Proposition G.6.10. — (The Class Equation) *Let $\mathcal{C}_{g_i}$ denote the conjugacy classes in a group G. Then*

$$\mathrm{Card}(G) = \mathrm{Card}(Z(G)) + \sum_{\mathrm{Card}(\mathcal{C}_{g_i})>1} \mathrm{Card}(\mathcal{C}_{g_i}).$$

Proof. — By Corollary 1.2.5 and the fact that the $\mathcal{C}_{g_i}$ are the orbits of G acting on itself by conjugation,

$$\operatorname{Card}(G) = \sum_{\mathcal{C}_{g_i}} \operatorname{Card}(\mathcal{C}_{g_i}).$$

By Lemma 1.2.14 d),

$$Z(G) = \bigcup_{\operatorname{Card}(\mathcal{C}_{g_i})=1} \mathcal{C}_{g_i}.$$

So

$$\begin{aligned}\operatorname{Card}(G) &= \sum_{\operatorname{Card}(\mathcal{C}_{g_i})=1} \operatorname{Card}(\mathcal{C}_{g_i}) + \sum_{\operatorname{Card}(\mathcal{C}_{g_i})>1} \operatorname{Card}(\mathcal{C}_{g_i}) \\ &= \operatorname{Card}(Z(G)) + \sum_{\operatorname{Card}(\mathcal{C}_{g_i})>1} \operatorname{Card}(\mathcal{C}_{g_i}).\end{aligned}$$

□