Notes: F.P. Greenleaf, 2000-08

Algebra I: Section 4. Transformation Groups

4.1 Actions of a group G on a space X.

Let G be a group and X a set.

4.1.1 Definition. *A* **group action** *is a map $\tau : G \times X \to X$ that assigns to each pair (g, x) in the Cartesian product set $G \times X$ an element $\tau(g, x) = g \cdot x$ in X. If we write $\tau_g(x) = g \cdot x$ we get a mapping $\tau_g : X \to X$ for each $g \in G$. We require the action to have the following properties.*

(1)
- (a) *For each $g \in G$, τ_g is a bijection. Hence $\tau_g \in \mathrm{Per}(X)$, the group of all permutation mappings on X.*
- (b) *For each $g_1, g_2 \in G$ we have $\tau_{g_1 g_2}(x) = \tau_{g_1}(\tau_{g_2}(x))$ – i.e. $g_1 g_2 \cdot x = g_1 \cdot (g_2 \cdot x)$. The latter property is what makes τ a* LEFT ACTION *(covariant action) on X; there is a similar definition for* RIGHT ACTIONS*, but they won't play a role in our discussion.*
- (c) *$\tau_e(x) = x$ for all $x \in X$, so that $\tau_e = \mathrm{id}_X$.*

It follows from (1) that each operator τ_g is invertible, and that $(\tau_g)^{-1} = \tau_{g^{-1}}$, because we have $\tau_g \circ \tau_{g^{-1}} = \tau_e = \mathrm{id}_X$. □

The τ_g are "transformations" of X. It follows from (1) that the map $\Phi : G \to (\mathrm{Per}(X), \circ)$ given by $\Phi(g) = \tau_g$ is a homomorphism from G to the group of permutations on X, in which the product is composition of operators: $\sigma_1 \circ \sigma_2(x) = \sigma_1(\sigma_2(x))$. The kernel of the homomorphism $\Phi : G \to \mathrm{Per}(X)$ is $\{g \in G : \tau_g = \mathrm{id}_X\}$. It is often referred to as the *kernel of the action* $G \times X \to X$, or simply the **action kernel**.

4.1.2 Definition. *Given a group action $G \times X \to X$, each point $x_0 \in X$ has a G-***orbit** $G \cdot x_0 = \{g \cdot x_0 : g \in G\}$. *We say that the action $G \times X \to X$ is* **transitive** *if there is just one orbit:*

(2) *For all $x, y \in X$, there exists a $g \in G$ such that $g \cdot x = y$*

or equivalently, $G \cdot x = X$ for any x. □

In X there is a natural an RST relation R such that

(3) $$x \sim_R y \iff \exists g \in G \text{ such that } y = g \cdot x$$

It is easily verified that R is reflexive, symmetric and transitive. Furthermore, the equivalence class of a point x_0 under R is precisely its G-orbit, so

(4) $$\begin{aligned} [x_0] &= \{y \in X : y \sim_R x_0\} \\ &= \{y \in X : \exists g \in G \text{ such that } y = g \cdot x_0\} \\ &= \{g \cdot x_0 : g \in G\} = (G\text{-orbit of } x_0) \end{aligned}$$

Thus X splits into *disjoint* G-orbits which fill X.

4.1.3 Exercise. Verify that the relation R defined in (3) is reflexive, symmetric, and transitive: (i) $x \sim_R x$, (ii) $x \sim_R y \Rightarrow y \sim_R x$, (iii) $x \sim_R y$ and $y \sim_R z \Rightarrow x \sim_R z$. □

4.1.4 Examples. Let G be any group.

(a) Take $X = G$ and $\tau_g(x) = gx$ (left translation by the element g). Clearly $\tau_{g_1 g_2}(x) = \tau_{g_1}(\tau_{g_2}(x))$ and $\tau_e(x) = x$, for all x. Each τ_g is a bijection on $X = G$ because $\mathrm{id}_G = \tau_e = \tau_g \circ \tau_{g^{-1}}$; obviously $(\tau_g)^{-1} = \tau_{g^{-1}}$. This is the action of G on *itself* by left translations. It is a *transitive action.* The action kernel is trivial because $\tau_g(x) = gx = x$ for all x implies (by cancellation) that $g = e$. $\square$

(b) Take $G = S_n$ (permutations on n objects) and $X = \{1, 2, \ldots, n\}$, with the obvious action of $\sigma \in S_n$ on the integers $1 \le k \le n$. (S_n is in fact *defined* as a group of transformations acting on this space X.) The action is transitive: given $i \neq j$ the two-cycle $\sigma = (i, j)$ satisfies $\sigma(i) = j$, but many other permutations work too. The action kernel, $\ker \Phi = \{\sigma \in S_n : \sigma(i) = i, \text{ all } i\}$, obviously reduces to the identity operator on X. $\square$

(c) The group of matrices $G = \mathrm{GL}(n, \mathbb{F}) = \{n \times n \text{ matrices } A : \det A \neq 0\}$ acts as $\mathbb{F}$-linear operators on the vector space $X = \mathbb{F}^n$ of n-tuples $\mathbf{x} = (x_1, \ldots, x_n)$ if we define

$$\tau_A(\mathbf{x}) = A\mathbf{x} \quad (\text{matrix product } (n \times n) \cdot (n \times 1)) \tag{5}$$

Since $\det A \neq 0$, τ_A is invertible and hence a bijection. It is obvious that $\tau_I = \mathrm{id}_X$ ($I = n \times n$ identity matrix) and $\tau_{AB} = \tau_A \circ \tau_B$. This action is *not* transitive. For one thing, the zero vector $\mathbf{0}$ has $A\mathbf{0} = \mathbf{0}$ for all A, so $G \cdot \mathbf{0} = \mathbf{0}$ is a single point. On the other hand if $\mathbf{x}_0 = \mathbf{e}_1 = (1, 0, \ldots, 0)$ it is not hard to construct linear operators that move $\mathbf{x}_0$ to any other nonzero vector $\mathbf{y}$; thus $G \cdot \mathbf{x}_0 = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{x} \neq \mathbf{0}\}$ is the only other orbit. $\square$

(d) Let G be the group of all rotations R_θ about the origin in $X = \mathbb{R}^2$. The operator R_θ rotates each vector $\mathbf{x}$ counterclockwise by θ radians. Recall that

$$\begin{aligned} R_{\theta'} &= R_\theta \quad \text{if and only if } \theta' = \theta + 2\pi k \text{ for some } k \in \mathbb{Z} \\ R_0 &= \mathrm{id}_X \quad \text{when } \theta = 0 \\ R_{\theta_1 + \theta_2} &= R_{\theta_1} \circ R_{\theta_2} \quad \text{for all } \theta_1, \theta_2 \in \mathbb{R} \\ R_{-\theta} &= (R_\theta)^{-1} \end{aligned}$$

Obviously G *cong*$\mathrm{SO}(2)$.
We have a group action because G is *defined* as a group of bijective linear transformations of $X = \mathbb{R}^2$, with composition as the group operation. The action is not transitive. There are two types of orbits:

$$\mathcal{O}_0 = G \cdot \mathbf{0} = \mathbf{0} \quad \text{(a one-point orbit)}$$
$$\mathcal{O}_r = \{\mathbf{x} : \|\mathbf{x}\| = r\} = G \cdot (r, 0) \quad \text{(a circle of radius } r > 0).$$

The action kernel is trivial. $\square$

(e) **Permutation action of G on a coset space G/H.** Here G is any group, H any subgroup, and $X = G/H =$ the space of cosets xH. We define a left action $G \times G/H \to G/H$ in the obvious way

$$\tau_g(xH) = gxH \qquad \tau_g : G/H \to G/H$$

The rules (1) are satisfied, and τ_g is a bijection because if we are given cosets xH, yH we get $\tau_g(xH) = \tau_g(yH) \Leftrightarrow gxH = gyH \Leftrightarrow xH = yH$ in G/H. The action is also transitive: given cosets xH, yH the group element $g = yx^{-1}$ moves xH to yH.

This action is called the *permutation representation* of G on G/H because the map $\Phi(g) = \tau_g$ is a homomorphism from G into the group of permutations $(\mathrm{Per}(G/H), \circ)$. This homomorphism can have nontrivial kernel, and hence different group elements $g_1 \neq g_2$ could produce the same effect on G/H. Two extreme cases are worth noting. If $H = G$ then $X = G/H$ consists of a single point and the action is not very interesting ($\ker\Phi = G$). If $H = \{e\}$ then $G/H = G$ and the permutation action becomes the action of G on itself by left translations, described above. $\square$

In a little while we will prove a remarkable result connecting algebra and geometry (Theorem 4.2.4):

> If $G \times X \to X$ is a *transitive* group action, there exists a subgroup $H \subseteq G$ such that the given action on X is really "equivalent to" – i.e. is a "disguised version of" – the permutation action $G \times G/H \to G/H$ on cosets of H. The latter action is defined, and can be studied, in purely algebraic terms.

We continue with some particularly important entries in our catalog of group actions, and prove some theorems leading up to an explanation of the preceeding comment.

4.1.5 Theorem (Cayley's Theorem). *If G is any finite group then G is isomorphic to some subgroup of the permutation group S_n, $n = |G|$.*

PROOF: The action of G on itself by left translations, $\tau_g(x) = gx$, gives a homomorphism $\Phi : G \to \mathrm{Per}(X)$ where $X = G$. Relabeling points in G as $g_1 = e, g_2, \ldots, g_n$, we can view this as a homomorphism $\Phi : G \to S_n$ where $X = \{1, 2, \ldots, n\}$. Each τ_g is a bijection. The kernel of the action is $\ker\Phi = \{g \in G : \tau_g = \mathrm{id}_X\}$. But $X = G$, and $\tau_g = \mathrm{id}_X \Leftrightarrow gx = x$ for all $x \Leftrightarrow g = e$. Hence $\ker\Phi$ is trivial and Φ is one-to-one. The range $H = \Phi(G)$ is a subgroup of S_n, and since Φ maps G one-to-one onto H we see that $G \cong H$ as required $\square$

We have shown that *all* finite groups are already present as subgroups of S_n for n sufficiently large. But S_n is a huge and unwieldy group, since $|S_n| = n!$ It may be possible to realize G within a smaller group of permutations: we could try the permutation action $G \times G/H \to G/H$ for suitably chosen subgroups $H \subseteq G$. (In Cayley's theorem we took $H = \{e\}$.) The map $\Phi : G \to \mathrm{Per}(G/H)$, $\phi(g) = \tau_g$, is always a homomorphism and its range $M = \Phi(G)$ is always a subgroup; Φ is an *isomorphism* making $G \cong M$ if and only if $\ker\Phi$ is trivial. To see when this happens we must compute $K = \ker\Phi$. That is an interesting calculation. Note that

$$\begin{aligned}
g \in \ker\Phi &\Leftrightarrow \tau_g(xH) = xH,\ \forall x \in G \Leftrightarrow gxH = xH,\ \forall x \in G \\
&\Leftrightarrow (x^{-1}gx) \cdot H = H,\ \forall x \in G \\
&\Leftrightarrow (x^{-1}gx) \in H,\ \forall x \in G \\
&\Leftrightarrow g \in xHx^{-1},\ \forall x \in G \\
&\Leftrightarrow g \in \bigcap_{x \in G} xHx^{-1}
\end{aligned}$$

The intersection is a subgroup M in G, being an intersection of subgroups; it is also normal in G. In fact $y(\bigcap_x xHx^{-1})y^{-1} = \bigcap_x (yx)H(yx)^{-1}$, but yx runs through all of G as x runs through G, so the last intersection is just $\bigcap_{z \in G} zHz^{-1} = M$. Hence $yMy^{-1} = M$ for any y and $M \lhd G$. Finally, note that $M \subseteq H$ because $H = eHe^{-1}$ is one of the groups in the intersection that defines M. This leads to the following natural identification of $M = \ker\Phi$.

(6) For the permutation action $G \times G/H \to G/H$, the action kernel $\ker\Phi$ is the *largest* subgroup M' in G such that: (i) M' is normal in G, (ii) $M' \subseteq H$. In particular, $\ker\Phi$ is trivial if and only if H contains no nontrivial subgroups M' that are normal in G.

[*Discussion:* Let $M = \bigcap_{x\in G} xHx^{-1}$; we claim that this is the largest group with properties (i), (ii). In fact, if M' is any subgroup having these properties, we have $x^{-1}M'x \subseteq M' \subseteq H$ for all x, hence $M' \subseteq xHx^{-1}$ for all x. Thus $M' \subseteq M = \bigcap_{x\in G} xHx^{-1}$, proving maximality of M.]

We resume our discussion of examples with one that will be of continuing interest.

4.1.6 Example (Adjoint action). Here we take $X = G$ and let G act on itself by **conjugation**:

$$\alpha_g(x) = gxg^{-1} \qquad \text{for all } x \in X = G$$

We have a group action because

$$\alpha_e = \mathrm{id}_G \qquad \alpha_{g_1g_2} = \alpha_{g_1} \circ \alpha_{g_2} \qquad \text{and hence} \qquad \alpha_{g^{-1}} = (\alpha_g)^{-1}$$

It is easily seen that each α_g is a bijection, and in fact is one of the inner automorphisms of G. Let $\Phi : G \to \mathrm{Int}(G) \subseteq \mathrm{Aut}(G)$ be the homomorphism $\Phi(g) = \alpha_g$. Note that

(i) Φ is trivial (with $\Phi(g) = \mathrm{id}_G$ for all g) if G is an abelian group.

(ii) In general, we have $\Phi(g) = \mathrm{id}_G \Leftrightarrow \alpha_g = \mathrm{id}_G \Leftrightarrow gxg^{-1} = x,\ \forall x \in G \Leftrightarrow gx = xg,\ \forall x \in G \Leftrightarrow g$ commutes with every element in G.

Recall the definition of the **center** of G: it is the subgroup $Z(G) = \{g \in G : gx = xg,\ \forall x \in G\}$.

4.1.7 Exercise. Prove that: (a) $Z(G)$ *is* a subgroup; (b) $Z(G)$ is normal in G; (c) $Z(G)$ is a "characteristic subgroup" in G – i.e. $\beta(Z(G)) = Z(G)$ for *every* automorphism $\beta \in \mathrm{Aut}(G)$, not just the inner automorphisms as in the definition of "normal subgroup". □

The preceeding remarks prove the following result

4.1.8 Theorem. *Under the adjoint action $G\times X \to X$, with $X = G$ and action $\alpha_g(x) = gxg^{-1}$, the action kernel for the homomorphism $\Phi : G \to \mathrm{Int}(G)$ is precisely the center $Z(G)$.*

4.1.9 Corollary. *For any group G we have* $\mathrm{Int}(G) \cong G/Z(G)$.

PROOF: The diagram at right commutes. Since $\ker\Phi = Z(G)$, which is also the kernel of the quotient homomorphism $\pi : G \to G/Z(G)$, it follows from the first isomorphism theorem that the homomorphism $\Phi : G \to \mathrm{Int}(G)$ induces an *isomorphism* $\tilde{\Phi} : G/Z(G) \to \mathrm{range}(\Phi)$. But $\mathrm{range}(\Phi) = \mathrm{Int}(G)$, by definition. Thus $G/Z(G) \cong (\mathrm{Int}(G), \circ)$. □

$$\begin{array}{ccc} G & \xrightarrow{\Phi} & \mathrm{Int}(G) \subseteq \mathrm{Aut}(G) \\ \pi\downarrow & \nearrow & \\ G/Z(G) & \tilde{\Phi} & \end{array}$$

Figure 4.1.

4.1.10 Exercise. Show that $\mathrm{Int}(G) = \{\alpha_g : g \in G\}$ is a *normal* subgroup in $\mathrm{Aut}(G)$.
Note: The quotient $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Int}(G)$ is often referred to as the group of **outer automorphisms** of G. □

Orbits under the adjoint action are called the **conjugacy classes** in G. Thus a typical conjugacy class is

$$C_x = \{gxg^{-1} : g \in G\} = \{\alpha_g(x) : g \in G\} = G \cdot x$$

In general the adjoint action is *not* transitive – for instance the class of the identity element is $\{e\}$. Thus G gets partitioned into disjoint conjugacy classes of various types. Some are trivial: the one-point classes. These include the identity element, but in fact we can identify all such classes.

(7) If $x \in G$, then $C_x = \{x\}$ (one-point class) $\Longleftrightarrow x \in Z(G)$ (the center of G)

This is immediate. The following less obvious observation has profound number-theoretic consequences.

4.1.11 Theorem (The Class Equation). *If G is finite and if $C_1 = C_e, C_2, \ldots, C_r$ are the distinct conjugacy classes, then*

$$\begin{aligned} |G| &= |C_1| + \ldots + |C_r| \\ &= \#(\textit{one-point classes}) + \sum_{\text{nontrivial } C_k} |C_k| \\ &= |Z(G)| + \sum_{\text{nontrivial } C_k} |C_k| \end{aligned} \tag{8}$$

Furthermore

(9) *If G is finite and C_x is any conjugacy class, the number of points $|C_x|$ in the class always divides $|G|$.*

PROOF: The statements in (8) are trivial; the claim in (9) will become obvious as we continue our discussion of general group actions, so we defer this part of the proof. □

Notice that $|Z(G)|$ is *nonzero* because the identity element lies in the center; this trivial fact will have serious implications, which is why all the one-point classes have been gathered together in the last version of the class equation.

4.2 Transitive group actions.

If a group a group action $G \times X \to X$ is not transitive, and $\mathcal{O}_{x_0}$ is any orbit in X, we may consider the action of G restricted to the orbit. The restricted action $G \times \mathcal{O}_{x_0} \to \mathcal{O}_{x_0}$ has the properties (1) required of a left action. Furthermore, by definition of *orbit* it is obvious that

The action of G on any orbit is a *transitive* action.

So X splits into disjoint pieces (orbits), on each of which the action is transitive. Thus the study of general group actions reduces to the study of transitive actions. However, as our examples show, G can have markedly different actions on different orbits.

For transitive actions there is a nice relation between algebra in the group and the geometry of the action, as we now explain.

4.2.1 Definition. *Let $G \times X \to X$ be any group action, and let x_0 be any point in X. The* **stabilizer** *of x_0 is the set $\mathrm{Stab}_G(x_0) = \{g \in G : g \cdot x_0 = x_0\}$ of points that leave x_0 fixed.* □

4.2.2 Exercise. Show that $\mathrm{Stab}_G(x_0)$ is a subgroup in G.
Note: These subgroups are generally *not* normal, and can vary erratically as x_0 runs through the space X. □

Now consider a transitive action (or more generally, the action of G on a single orbit in some larger space).

4.2.3 Theorem. *If G is finite and $G \times X \to X$ is a transitive group action, then the space X must be finite. Furthermore, if we fix a base point $x_0 \in X$ and let $H = \mathrm{Stab}_G(x_0)$, we have*

$$|X| = |G/H| \qquad \textit{and} \qquad |G| = |G/H| \cdot |H| = |X| \cdot |\mathrm{Stab}_G(x_0)| \tag{10}$$

In particular, for transitive actions $|X|$ must always divide $|G|$.

4.2.4 Corollary. *If C_x is a conjugacy class in a finite group G (an orbit under the adjoint action), then the cardinality $|C_x|$ of the class must divide $|G|$.*

PROOF (4.2.3): Let $H = \mathrm{Stab}_G(x_0)$. There is a bijective correspondence between $G/H = \{xH : x \in G\}$ and points in X. It is implemented by the following map:

$$\psi : G/H \to X \qquad \text{where} \qquad \psi(gH) = g \cdot x_0 \tag{11}$$

This map is well-defined – i.e. if we take a different coset representative g' such that $g'H = gH$, we still get $\psi(g'H) = \psi(gH)$. [We have $g'H = gH \Leftrightarrow$ there is some $h \in H$ such that $g' = gh$. But then we get

$$g' \cdot x_0 = (gh) \cdot x_0 = g \cdot (h \cdot x_0) = g \cdot x_0 \quad ,$$

since $h \cdot x_0 = x_0$ by definition of $H = \mathrm{Stab}_G(x_0)$.]

Furthermore ψ is an *onto* map because the action is transitive. [Given $y \in X$ there is some $g \in G$ such that $y = g \cdot x_0$, and then $\psi(gH) = g \cdot x_0 = y$.] Finally, ψ is a *one-to-one* map (and $\psi : G/H \to X$ is a bijection). In fact, if $\psi(g_1H) = \psi(g_2H)$ we have $g_1 \cdot x_0 = g_2 \cdot x_0$, which implies that $g_1^{-1} \cdot (g_2 \cdot x_0) = (g_1^{-1}g_2) \cdot x_0 = x_0$. But $g_1^{-1}g_2$ fixes $x_0 \Leftrightarrow g_1^{-1}g_2 \in H$; thus there exists an $h \in H$ such that $g_1^{-1}g_2 = h$, and hence $g_2H = (g_1h)H = g_1H$ as required.

Since ψ is a bijection we must have $|X| = |G/H|$. Once we know this we finish the proof by applying Lagrange's theorem, which says that $|G| = |G/H| \cdot |H|$ for any subgroup. $\square$

There is a lot more to be said about the bijection $\psi : G/H \to X$ we have constructed in the proof of 4.2.3. Consider the diagram at right. As above, we start with a transitive action $G \times X \to X$, fix a base point $x_0 \in X$, define $H = \mathrm{Stab}_G(x_0)$, and define the bijection ψ via $\psi(gH) = g \cdot x_0$. A group element $g \in G$ acts on X as some operator τ_g. On G/H we also have a transitive action of G, the permutation action discussed earlier, which is implemented by the operators

$$\begin{array}{ccc} G/H & \xrightarrow{\psi} & X = G \cdot x_0 \\ L_g \downarrow & & \downarrow \tau_g \\ G/H & \xrightarrow{\psi} & X \end{array}$$

Figure 4.2

$$L_g(xH) = gxH \quad \text{for } g, x \in G \qquad (L_g : G/H \to G/H) \tag{12}$$

We claim that the diagram in Figure 4.2 is *commutative*, which means that

$$\psi \circ L_g = \tau_g \circ \psi \qquad (\text{or equivalently, that } \ \tau_g = \psi \circ L_g \circ \psi^{-1}, \ \forall g \in G) \tag{13}$$

The property is easily checked: for any coset yH we have

$$\tau_g(\psi(yH)) = \tau_g(y \cdot x_0) = g \cdot (y \cdot x_0) = (gy) \cdot x_0 = \psi(gyH) = \psi(L_g(yH))$$

and therefore $\tau_g \circ \psi = \psi \circ L_g$ as maps from G/H to X. Property (13) is often described by saying that the map $\psi : G/H \to X$ *intertwines* the actions of G on the two spaces, or that ψ is an *equivariant* map. We summarize all this as follows.

4.2.5 Theorem. *Let $G \times X \to X$ be a transitive group action, fix a base point $x_0 \in X$, let $H = \mathrm{Stab}_G(x_0)$, and define the bijection $\psi : G/H \to X$ as in* (12)*. Then ψ intertwines the two group actions and the diagram shown in Figure 4.2 commutes.*

The identity $\tau_g = \psi \circ L_g \circ \psi^{-1}$ says that we get the same result following two different paths:

- Transfer $x \in X$ over to a coset in G/H
- Act on the coset via L_g
- Transfer the result back to X

$\Big\}$ = (the original action of τ_g on x)

What all this means in practice is that there is a way to identify points in G/H with points in X so that the action of L_g on G/H becomes the action of τ_g on X. Intuitively, the actions $L : G \times G/H \to G/H$ and $\tau : G \times X \to X$ are the *same action in different disguises.* They are "isomorphic" group actions, in the same sense that certain groups are isomorphic. (The notion of "isomorphism" applies to all sorts of algebraic structures.) The following example illustrates this notion of isomorphic actions.

4.2.6 Example. The matrix group SO(3) consists of all real orthogonal 3×3 matrices with

$\det(A) = 1$. A matrix A is *orthogonal* if $A^{\mathrm{t}}A = I = AA^{\mathrm{t}}$ (A^{t} = transpose matrix), and then $A^{\mathrm{t}} = A^{-1}$. Given $A \in \mathrm{SO}(3)$ we get a linear operator

$$\tau_{_A} : \mathbb{R}^3 \to \mathbb{R}^3 \quad \text{via} \quad \tau_{_A}(\mathbf{v}) = A\mathbf{v} \quad \text{(a matrix product } (3\times 3)\cdot(3\times 1)\text{)}.$$

It is well known from linear algebra that the resulting group G of linear operators on $\mathbb{R}^3$ consists of all rotations $R_{\mathbf{u},\theta}$ with $\theta \in \mathbb{R}$, $\mathbf{u}$ a vector with length $\|\mathbf{u}\| = 1$,

$$R_{\mathbf{u},\theta} = \begin{pmatrix}\text{Rotation counterclockwise by } \theta \text{ radians}\\ \text{about the axis through the origin deter-}\\ \text{mined by the unit vector } \mathbf{u}\end{pmatrix}$$

As usual, multiplication of matrices corresponds to composition of rotation operators:

$$\tau_{_{AB}} = \tau_{_A} \circ \tau_{_B} \qquad \tau_{_I} = \mathrm{id}_{\mathbb{R}^3} \qquad (\tau_{_A})^{-1} = \tau_{_{A^{-1}}} = \tau_{_{A^{\mathrm{t}}}}$$
$$\tau_{_A} = \tau_{_B} \text{ on } \mathbb{R}^3 \iff A = B \text{ as matrices}$$

Next consider the unit sphere in $\mathbb{R}^3$, $X = \{\mathbf{x} \in \mathbb{R}^3 : \|\mathbf{x}\| = 1\}$, where $\|\mathbf{x}\|^2 = x_1^2 + x_2^2 + x_3^2$. Every rotation $\tau_{_A}$ maps X to itself, and we get a group action $G \times X \to X$

4.2.7 Exercise. Explain why this action is transitive.
Hint: Use geometric reasoning to show that the unit vector $\mathbf{e}_3 = (0,0,1)$ can be moved by a rotation to any desired position on the sphere. (By what angle about what axis?) □

Take $\mathbf{x}_0 = (0,0,1)$ in X. The stabilizer $H = \mathrm{Stab}_G(\mathbf{x}_0)$ consists of all rotations (by any angle θ) about the positive z-axis; the corresponding group of matrices in SO(3) is

$$H = \left\{ \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} : \theta \in \mathbb{R} \right\}$$

By our discussion, there is a bijection between G/H (a purely algebraic construct) and the sphere X, given by $\psi(AH) = A\mathbf{x}_0$. This bijection transfers the purely algebraic action $L_{_A} : G/H \to G/H$ to the geometric action $\tau_{_A} : X \to X$. Thus the geometric action of SO(3) on the sphere can be studied by algebraic methods by examining the action $G \times G/H \to G/H$. □

4.2.8 Exercise. Compute the stabilizer $H = \mathrm{Stab}_G(\mathbf{x}_0)$ above and show it has the form stated.
Hint: A rotation about the origin in $\mathbb{R}^2$ is described by a matrix $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ for suitably chosen θ. □

4.2.9 Exercise. Let X be the unit circle $\{z \in \mathbb{C} : |z| = 1\}$. The group $G = (\mathbb{R}, +)$ acts on X via rotations

$$\tau_\theta(z) = e^{2\pi i\theta} \cdot z = (\cos\theta + i\sin\theta)\cdot z$$

Verify that this is a group action. Taking base point $z_0 = 1 + i0$ in X, compute $H = \mathrm{Stab}_G(z_0)$. Does the coset space G/H look familiar? □

4.2.10 Exercise. Consider the action $S_n \times X \to X$ of the permutation group on $X = \{1, 2, \ldots, n\}$. This action is transitive (why?). Suppose we fix the base point $x_0 = 1$. Determine the stabilizer subgroup $H = \mathrm{Stab}_{S_n}(x_0)$ and explain why it is isomorphic to S_{n-1}. What happens if you take some other base point $x_0 = k$ in X? □

4.2.11 Exercise. The group $G = \mathrm{SL}(n, \mathbb{R})$ acts on $X = \mathbb{R}^n$. It leaves the origin $\mathbf{0}$ fixed, and hence leaves invariant the complementary set $Y = X \sim \{\mathbf{0}\}$. If $n \geq 2$ is the action $G \times Y \to Y$ transitive? I.e. is Y a single G-orbit, or does it break up into smaller orbits?
Note: At the beginning of Section 3.1 we considered the action of $\mathrm{GL}(n, \mathbb{R})$ on $\mathbb{R}^n$, which *does*

act transitively on Y. The present case is more subtle, and the action on Y fails to be transitive when $n = 1$. (What are the orbits in this case?) $\square$

4.3 Applications of the Conjugacy Class Equation.

Consider the action $G \times X \to X$ where a group G acts on itself by conjugation, via $\alpha_g(x) = gxg^{-1}$. We have seen that the cardinality $|C_x|$ of an orbit (conjugacy class) divides the order of G, and in fact that

$$|C_x| = \frac{|G|}{|Z_{_G}(x)|} \qquad \text{where } Z_{_G}(x) \text{ is the "centralizer of } x\text{"} \ = \{g \in G : gxg^{-1} = x\} \tag{14}$$

It is easily verified that the centralizer $Z_{_G}(x)$ of any group element is a subgroup of G; in fact it is just the stabilizer of x under conjugation. Using this terminology we may recast the class equation 4.1.11 in a slightly different form.

4.3.1 Corollary (Class Equation). *If G is a finite group and S a set of representatives for the distinct conjugacy classes in G, then*

$$|G| = |Z(G)| + \sum_{x \in S'} \frac{|G|}{|Z_{_G}(x)|} = |Z(G)| + \sum_{x \in S'} |C_x| \tag{15}$$

where S' is the set of representatives of the conjugacy classes such that $|C_x| > 1$.

We note that an element $a \in G$ lies in the center $Z(G) \Leftrightarrow \alpha_g(a) = a, \ \forall g \in G \Leftrightarrow Z_{_G}(a) = \mathrm{Stab}_G(a)$ is all of G. As a simple application we show how the class equation can be used to reveal some internal structure in a finite group. We already know that $G \cong (\mathbb{Z}_p, +)$ if $|G| = p$ is a prime. When $|G| = p^n$ (a power of some prime $p > 1$), the group still has some abelian aspects.

4.3.2 Theorem (Cauchy). *Let G be a finite group with $|G| = p^n$ for some prime $p > 1$ and some $n \geq 1$. Then the center is nontrivial: $Z(G) \neq \{e\}$.*

Proof: Obviously $e \in Z(G)$. What else can lie in the center? Look at the centralizer $Z_{_G}(a) = \{g \in G : gag^{-1} = a\}$. If $a \neq e$ then $|Z_{_G}(a)| \geq 2$ since $\{e, a\} \subseteq Z_{_G}(a)$; but $|Z_{_G}(a)|$ divides $|G| = p^n$, by Lagrange, so there is an integer $1 \leq k(a) \leq n$ such that $|Z_{_G}(a)| = p^k$. Furthermore, a class C_a is nontrivial $\Leftrightarrow |Z_{_G}(a)| < |G| \Leftrightarrow k(a) < n$. Thus if C_a is nontrivial we have $1 < |Z_G(a)| < |G|$ and the exponent $k(a)$ must satisfy $0 < k(a) < n$.

The class equation (15) says

$$p^n = |Z(G)| + \sum_{a \in S'} \frac{p^n}{p^{k(a)}}$$

and it follows that

$$|Z(G)| = p^n - \sum_{a \in S'} \frac{p^n}{p^{k(a)}}$$

Since $k(a) < n$ for each $a \in S'$, the right side is divisible by p, so p divides $|Z(G)|$ – i.e. $|Z(G)| = \ell p$ for some $\ell \geq 1$. In particular $|Z(G)| > 1$, as required. $\square$

4.3.3 Corollary. *If $|G| = p^2$ for some prime $p > 1$, then G is abelian.*

Proof: By 4.3.2, the center $Z(G)$ is nontrivial. By Lagrange's theorem, the only remaining possibilities are: $|Z(G)| = p$ or p^2. If $|Z(G)| = p^2$ we're done. If $|Z(G)| = p$, there would exist some $a \in G \sim Z(G)$, and for this element we would have $Z_{_G}(a) \supseteq Z(G)$ and $|Z_{_G}(a)| \neq |Z(G)|$ because the centralizer also contains a. That forces $Z_{_G}(a) = G$, which means that a is in the center of G, violating our hypothesis that $a \notin Z(G)$. This contradiction shows that the case $|Z(G)| = p$ cannot occur. $\square$

It follows that all groups of order $1, 4, 9, 25, \ldots$ are abelian. In Cahpetr 3 we showed "by hand" that this is true when $|G| = 4$, such a direct proof by brute force would be much harder for groups of order $|G| = 9$; none of the ideas used when $|G| = 4$ carry over.

We now prove a result that relates the internal structure of a finite group to the primes $p > 1$ that divide the order of the group. This result is simple to state but not so easy to prove. We will attack it in two stages, first proving the result for finite *abelian* groups, and then for general finite groups.

4.3.4 Theorem (Cauchy's Theorem for Abelian Groups). *Let G be a finite abelian group. If $p > 1$ is a prime that divides $n = |G|$, then there is an element $a \in G$ of order exactly equal to p – i.e. G contains an isomorphic copy of $(\mathbb{Z}_p, +)$.*

PROOF: We argue by induction on n. The result is true by default if $n = 1$. (There are no prime divisors $p > 1$ of a group with $|G| = 1$, so you can't exhibit a prime p for which the claim fails to be true.) For $n = 2$, G is isomorphic to $(\mathbb{Z}_2, +)$ whose nontrivial element has order 2. Thus we may assume $n \geq 3$. We procede to the induction step: for $n \geq 3$ we assume the result true for any groups G' of order less than n and any prime $p > 1$ that divides $|G'|$; we must prove the result holds true any group G of order n. We distinguish several possibilities.

Case 1: G has no proper subgroups H. "Proper" means: $H \neq \{e\}$ and $H \neq G$. Since $n > 1$ there is an element $a \in G$ such that $a \neq e$. The cyclic subgroup $H = \langle a \rangle$ it generates must equal G, so G is cyclic with $G \cong (\mathbb{Z}_n, +)$. But if n is not prime it is easy to find proper subgroups in $\mathbb{Z}_n$, so n must be a prime and $p = n$ is its only prime divisor. The generator a has $o(a) = p$, as required.

4.3.5 Exercise. If $n > 1$ explain why there must exist *proper* subgroups $(e) \neq H \neq G$ in the cyclic group $G = (\mathbb{Z}_n, +)$. □

Case 2: There is a proper subgroup N. The subgroup N is abelian and $1 < |N| < |G| = n$, so the induction hypothesis applies to N. If p divides $|N|$, we can find an element of order p within N, and the proof is finished. Thus we may assume that p *does not* divide $|N|$.

Since G is abelian, N is a normal subgroup, and the quotient group G/N is also abelian; both have order less than n. By Lagrange's theorem we have $|G| = |N| \cdot |G/N|$, and since p does not divide $|N|$ it must divide $|G/N|$. The induction hypothesis applies to G/N, so there must be an element $\overline{a} \in G/N$ of order p; in particular $\overline{a} \neq \overline{e}$ (the identity element in G/N). The quotient map $\pi : G \to G/N$ is surjective, so we can find a preimage $a \in G$ such that $\pi(a) = \overline{a}$. But π is a homomorphism, so we must have $a^p \in N = \ker(\pi)$ because $\pi(a^p) = (\pi(a))^p = \overline{a}^p = \overline{e}$, which implies that $a^p \in \ker \pi = N$.

Thus $a^p \in N$, but $a \notin N$ because that would imply $\overline{a} = \pi(a) = \overline{e}$, contrary to our assumption that $\overline{a} \neq \overline{e}$. One corollary to Lagrange's theorem says:

> Every element in a finite group G' satisfies the condition $y^{|G'|} = e$.

In our present context that means $(a^p)^{|N|} = e$ since $a^p \in N$. But then we conclude that

$$(a^{|N|})^p = a^{(p|N|)} = (a^p)^{|N|} = e$$

Let $b = a^{|N|}$. Obviously $b^p = e$, but the only powers of a group element b that equal e are multiples of its order $o(b)$, so p must be a multiple of $o(b)$. Since $p > 1$ is prime there are just two possibilities: either $o(b) = p$, in which case we have found the desired element of order p, or $o(b) = 1$ which means that $b = e$.

In the latter case we have $a^{|N|} = e$, hence in the quotient group we have $\overline{a}^{|N|} = \overline{e}$. But $\overline{a}$ had order p, by definition, which means $|N|$ must be a multiple of p. That is a contradiction because we know that p does not divide $|N|$. Conclusion: the case $b = e$ cannot arise, and the proof is complete. □

We now turn to the proof for general (not necessarily abelian) groups. It will make essential use of the previous result, as well as the Class Equation 4.3.1 for conjugacy classes (which is

only meaningful for nonabelian groups).

4.3.6 Theorem (Cauchy). *Let G be a finite group. If $p > 1$ is a prime that divides $n = |G|$, then there is an element $a \in G$ of order exactly p.*

PROOF: If $n = 1$ the group is trivial and the result is true by default, as noted in 4.3.4; if $n = 2$ the element a such that $a \neq e$ satisfies $a^2 = e$, so $G \cong \mathbb{Z}_2$ is abelian and our result is true. In proving the inductive step we may assume $n \geq 2$. The induction hypothesis says:

> *Induction hypothesis* $P(n)$: If G' is any group such that $|G'| \leq n$, and if $p > 1$ is a prime that divides the order of G', then then there is an element $a \in G'$ of order $o(a) = p$.

Assuming $P(n)$ true we must prove $P(n+1)$ is true. So, assume G is a nontrivial group such that $|G| \leq n+1$ and that $p > 1$ is a prime divisor of $|G|$. There are several possibilities.

Case 1: $|G| \leq n$. The induction hypothesis applies to G, and there is an element of order $o(a) = p$.

Case 2: $|G| = n+1$ *and there is a proper subgroup H in G such that p divides $|H|$.* The induction hypothesis applies to H; there is an element in H such that $o(a) = p$.

Case 3: $|G| = n+1$ *and p does not divide the order of any proper subgroup in G.* Consider the center $Z(G)$. If $Z(G) = G$ we are in the abelian case considered previously, and can head for the exit. Otherwise there are elements $a \notin Z(G)$ and we may consider their centralizer subgroups $Z_{_G}(a) = \{g \in G : ga = ag\}$. Now $Z_{_G}(a) \neq G$ because a is not central, and $Z_{_G}(a) \neq \{e\}$ because it includes both a and e, so $Z_{_G}(a)$ is a *proper* subgroup in G whenever $a \notin Z(G)$. Let S' be a set of representatives for the nontrivial conjugacy classes (those containing more than one point). These representatives lie outside the center, so by Theorem 4.2.3 we get

$$|C_a| = |G|/|Z_{_G}(a)| > 1, \ \forall a \in S'.$$

The class equation says

$$|G| = |Z(G)| + \sum_{a \in S'} \frac{|G|}{|Z_{_G}(a)|} = |Z(G)| + \sum_{a \in S'} |C_a|$$

By the hypotheses prevailing in *Case 3*, p is not a divisor of $|Z_{_G}(a)|$ for any $a \notin Z(G)$ because these are all proper subgroups. But p does divide $|G|$, so p divides $|C_a| = |G|/|Z_{_G}(a)|$ for each $a \in S'$. It follows that

$$p \ \text{ divides } \ |Z(G)| = |G| - \sum_{a \in S'} |C_a|$$

We have a contradiction if $Z(G)$ is a proper subgroup; since we already know that $Z(G) \neq G$, the only way out is to have $Z(G)$ trivial. But that is also impossible: we can't have $|Z(G)| = 1$ because p divides $|Z(G)|$ and $p > 1$.

To summarize what has happened in *Case 3*: If $Z(G) = G$ we are in the abelian case, and if $Z(G) \neq G$ we get a contradiction. Since all cases have been addressed, the inductive proof of the theorem is complete. □

4.3.7 Exercise. Let G be a finite group and let $g \in G$. Explain why the only powers g^m that are equal to e are multiples of the order $o(g)$. □