18.10.1 Let S be a G-set, $s_1, s_2 \in S$. Suppose that there exists an $x \in G$ such that $s_2 = x * s_1$, i.e., $s_2 \in G * s_1$. Show that $G_{s_2} = xG_{s_1}x^{-1}$.

Solution Let $x \in G$ and $y \in G_{s_2}$. Then

$$x^{-1}yx * s_1 = x^{-1}y * s_2 = x^{-1} * s_2 = s_1,$$

so $x^{-1}yx \in G_{s_1} \implies y \in xG_{s_1}x^{-1}$.

Now let $xyx^{-1} \in xG_{s_1}x^{-1}$, which gives

$$xyx^{-1} * s_2 = xy * s_1 = s_2,$$

so $yx^{-1} \in G_{s_2}$. Thus, $G_{s_2} = xG_{s_1}x^{-1}$.

18.10.2 Let S be a G-set. We say that the G-action is *transitive* if for all $s_1, s_2 \in S$, there exists a $g \in G$ satisfying $g * s_1 = s_2$, equivalently, $S = G * s$; and is *doubly transitive* if for all pairs of elements (s_1, s_1') and (s_2, s_2') in S with $s_1 \neq s_1'$ and $s_2 \neq s_2'$, there exists a $g \in G$ satisfying $g * s_1 = s_2$ and $g * s_1' = s_2'$. Suppose that S and G are finite. Show if the action is transitive then $|G| \geq |S|$ and if the action is doubly transitive then $|G| \geq |S|^2 - |S|$.

Solution Let the action on S be transitive.

Since $|G * s| = [G : G_s]$, by Lagrange, we have $|G| = |G * s||G_s| \geq |G * s| = |S|$, as desired.

Now let the action be doubly transitive.

Pick any s_1 and s_1' in S. There are $|S|(|S| - 1)$ ways to do this since they must be distinct. Then for any s_1', s_2' different from s_1 and s_2, respectively, there exists g so that $g * s_1 = s_2$ and $g * s_1' = s_2'$. If we change s_1' and s_2', then we must get a different value of g, which means that there has to be at least one different g for each pair s_1, s_1', so $|G| \geq |S|^2 - |S|$.

20.26.1 Let G be a group. Show all of the following:

a. $Z(G) = \bigcap_{a \in G} Z_G(a)$.

b. $a \in Z(G)$ if and only if $C(a) = \{a\}$ if and only if $|C(a)| = 1$.

c. $a \in Z(G)$ if and only if $G = Z_G(a)$.

d. If G is finite, then $a \in Z(G)$ if and only if $|Z_G(a)| = |G|$.

Solution a. Let $z \in Z(G)$. Then clearly $z \in \bigcap_{a \in G} Z_G(a)$, since z commutes with everything.
Let $z \in \bigcap_{a \in G} Z_G(a)$. Then for all $g \in G$, $z \in Z_G(g)$, so $zg = gz$. Thus, $z \in Z(G)$.

b. The second equivalence is clear, since $a \in C(a)$.
Let $a \in Z(G)$. Then $ax = xa \iff a = xax^{-1}$ for all $x \in G$. Thus,

$$C(a) = \{xax^{-1} \mid x \in G\} = \{a\},$$

as desired.
Let $C(a) = \{a\}$. Then $xax^{-1} = a$ for all $x \in G$, by definition of the set, so the equivalence holds.

c. Let $a \in Z(G)$ so that $ax = xa$ for all $x \in G$. Then $G \subseteq Z_G(a) \subseteq G$, so equality holds.
Let $G = Z_G(a)$, so that $ax = xa$ for all $x \in G$. This is equivalent to saying $a \in Z(G)$ by definition, since

$$Z(G) = \{x \in G \mid xy = yx \text{ for all } y \in G\}.$$

d. "$\implies$" holds because of part (c).
Let $|Z_G(a)| = |G|$. Since $Z_G(a) \subseteq G$, this implies that $G = Z_G(a)$, so by (c), "$\impliedby$" holds.

20.26.2** Let G be a group and $k(G)$ the number of conjugacy classes in G. Suppose that G is finite. Show that $k(G) = 3$ if and only if G is isomorphic to the cyclic group of order three or the symmetric group on three letters.

Solution The backwards implication is clear. $\mathbb{Z}/3\mathbb{Z}$ has three elements and it's abelian, so its conjugacy classes are exactly the elements of $\mathbb{Z}/3\mathbb{Z}$. For S_3, this can be seen by direct computation.

If G is abelian, then $G \simeq \mathbb{Z}/3\mathbb{Z}$. Indeed, the orbit of each element is itself, and we have three conjugacy classes,

If G isn't abelian, then write $|G| = 1 + a + b$, where a and b are the sizes of the non-trivial conjugacy classes with $a \leq b$.

By Lagrange, we know that $a \mid |G|$ and $b \mid |G|$, so $a \mid b+1$ and $b \mid a+1$. Thus, for some $\alpha, \beta \in \mathbb{Z}$

$$\beta b = a + 1 \quad \text{and} \quad \alpha a = b + 1.$$

The following case follow from these equations:

$b = 3$:

In this case, $a = 2$ or 1, from the second equation. But if $a = 1$, then $a + 1 < \beta b$, so we can only have $a = 2$. Thus, $|G| = 6$. By Cauchy's theorem, since a and b are prime and divide $|G|$, there exist elements of order 2 and 3 in G, which means that $G \simeq S_3$.

$b = 2$:

Then $a = 1$ or $a = 3$ from the second equation. But we assumed $a \leq b$, so we have $a = 1$. In this case, $|G| = 4$. But groups of order 4 are abelian. If it has an element of order 4, then this is clear. If it has two elements x, y of order 2, then

$$xy(xy) = e \implies xy = y^{-1}x^{-1} = yx.$$

It cannot have an element of order 2 and two elements of order 1, so we're done with this case.

$b = 1$:

Then $a = 1$ since we assumed $a \leq b$, which gives $|G| = 3$. In this case, for any two elements x, y in G, $xyx^{-1} = y \implies xy = yx$, since the conjugacy classes are singletons. Thus, $G \simeq \mathbb{Z}/3\mathbb{Z}$ in this case.

20.26.5 Compute all the conjugacy classes and isotropy subgroups in A_4.

Solution We can think of the elements of A_4 with swapping columns on an $n \times n$ matrix an even number of times.

Then the conjugacy class of e is given by $\{e\}$.

The conjugacy class of $\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}$ is

$$\{\begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix}\},$$

the conjugacy class of $\begin{pmatrix}1 & 2 & 3\end{pmatrix}$ is

$$\{\begin{pmatrix}1 & 2 & 3\end{pmatrix}, \begin{pmatrix}2 & 4 & 3\end{pmatrix}, \begin{pmatrix}1 & 3 & 4\end{pmatrix}, \begin{pmatrix}1 & 4 & 2\end{pmatrix}\},$$

and the conjugacy class of $\begin{pmatrix}1 & 3 & 2\end{pmatrix}$ is

$$\{\begin{pmatrix}1 & 3 & 2\end{pmatrix}, \begin{pmatrix}2 & 3 & 4\end{pmatrix}, \begin{pmatrix}1 & 4 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 4\end{pmatrix}\}.$$

To find the stabilizer, we just need to find the center of the group. The center of the group are the singleton conjugacy classes, which is simply the identity, so A_4 has a trivial stabilizer.

20.26.6** Let G be a group of order p^n, p a prime. Suppose the center of G has order at least p^{n-1}. Show that G is abelian.

Solution The center of G is a subgroup of G, so if $Z(G)$ has order p^n, $Z(G) = G$, so G commutes. Assume from now on that $Z(G)$ has order p^{n-1}.

Recall that the center of a group is normal, so $G/Z(G)$ has a group structure. By Lagrange, we know that

$$|G| = |G : Z(G)||Z(G)| \implies |G/Z(G)| = |G|/|Z(G)| = p.$$

By Cauchy's theorem, $G/Z(G)$ has an element of order p, so $G/Z(G) \simeq \mathbb{Z}/p\mathbb{Z}$. In particular, there exists an element $g \in G \setminus Z(G)$ such that

$$g^p Z(G) = Z(G),$$

so $g^p \in Z(G)$. Since $g \in G \setminus Z(G)$, this means that $g^k \in G \setminus Z(G)$ for $1 \le k < p$, and $g^p = e$. Indeed, g must have order p. Otherwise, $|G \setminus Z(G)| > p$ which can't happen, or if g has order 1, it is the identity, which is in the center.

This means that g generates $G \setminus Z(G)$. So, elements in $G \setminus Z(G)$ must commute with themselves, and $Z(G)$ commutes with everything, so G is abelian.

20.26.9 Suppose that H is a proper subgroup of a finite group G. Show that $G \neq \bigcup_{g \in G} gHg^{-1}$.

Solution Notice that if $gHg^{-1} = kHk^{-1}$, we have

$$H = g^{-1}kH(g^{-1}k)^{-1} \iff g^{-1}k \in N_G(H) \implies gN_G(H) = kN_G(H).$$

Thus, we get a bijection $gN_G(H) \mapsto gHg^{-1}$, which means that the number of conjugates of H is equal to $[G : N_G(H)]$, which is clearly at most $[G : H]$ since $H \subseteq N_G(H)$.

Since each conjugate gHg^{-1} contains e,

$$\left| \bigcup_{g \in G} gHg^{-1} \right| = [G : N_G(H)]|H| - (n-1) \le [G : H]|H| - (n-1) = |G| - (n-1) < |G|,$$

so we cannot have equality.

20.26.10 Let H be a subgroup of G. Let H act on G/H by translation. Compute the orbits, stabilizers, and fixed points of this action.

Solution Consider $gH \in G/H$, and let $h_1, h_2 \in H$. Then

$$(h_2 h_1^{-1}) h_1 gH = h_2 gH,$$

which means that there is only one orbit, since every element of H is equivalent to each other with the orbit equivalence class.

Let $h \in H$ be a stabilizer. Then by definition, for all $g \in G$, we have $hgH = gH$. Thus, $g^{-1}hgH = H$, which means that $g^{-1}hg \in H \implies h \in gHg^{-1}$. So our stabilizers are all the conjugates of H.

Let $gH \in G/H$. If $g \in H$, then take a point $g' \in G \setminus H$. Then $g' * gH = g'H \neq H$. Otherwise, $g^{-1} * gH = H \neq gH$, so there are no fixed points.

20.26.16 Let p be an odd prime. Classify all groups G of order $2p$ up to isomorphism.

Solution If G has an element of order $2p$, then $G \simeq \mathbb{Z}/2p\mathbb{Z}$.

By Cauchy's theorem, since $2, p \mid 2p$, G has an element a of order 2 and an element b of order p.

If ab has order $2p$, then $G \simeq \mathbb{Z}/2p\mathbb{Z}$.

If ab has order p, then $ab \in \langle b \rangle$, since there is no room for another subgroup of order p, but this implies that $a \in \langle b \rangle$, which can't happen.

If ab has order 2, then $abab = e \implies ab = b^{-1}a$, in addition to $a^2 = b^p = e$, so $G \simeq D_p$.

20.26.17 Let S be a G-set. Suppose that both S and G are finite. If $x \in G$, define the *fixed point set* of x in G by

$$F_S(x) \coloneqq \{s \in S \mid x * s = s\}.$$

Show that the number of orbits N of this action satisfies

$$N = \frac{1}{|G|} \sum_G |F_S(x)|.$$

Solution We first consider the set

$$C = \{(g, s) \mid g * s = s\}.$$

Notice that $|C| = \sum_{x \in G} |F_S(x)|$ and that $|C| = \sum_{s \in S} |G_s|$. We can think of this as analogous to changing the index on a double sum.

Indeed, if we fix g and sum over the values of s with $(g, s) \in C$, then we get $|F_S(g)|$. Similarly, if we fix s and sum over g, we get $|G_s|$, so the two sums are equivalent.

So, we have

$$\sum_{x \in G} |F_S(x)| = \sum_{s \in S} |G_s|.$$

We can decompose S into its disjoint orbits, so the sum is the same as

$$\sum_{i=1}^{N} \sum_{s \in \text{orbit } i} |G_s|.$$

By a theorem, we know that $|G_s||G * s| = |G|$, so if we sum $|G_s|$ over the elements of the orbit, we get

$$\sum_{i=1}^{N} \sum_{s \in \text{orbit } i} |G_s| = N|G|.$$

Thus, dividing by $|G|$, we get

$$N = \frac{1}{|G|} \sum_G |F_S(x)|$$

as desired.