Lemma:

(a) For all $g' \in G$ we have that $\mathrm{Fix}(g'g(g')^{-1}) = g' \cdot \mathrm{Fix}(g) \coloneqq \{g' \cdot x \in X : g \cdot x = x\}$.

Proof:

$$\begin{aligned} x \in \mathrm{Fix}(g'g(g')^{-1}) &\iff (g'g(g')^{-1}) \cdot x = x \\ &\iff g \cdot ((g')^{-1} \cdot x) = (g')^{-1} \cdot x \\ &\iff (g')^{-1} \cdot x \in \mathrm{Fix}(g) \iff x \in g' \cdot \mathrm{Fix}(g). \end{aligned}$$

(b) For all $g \in G$ we have that $G_{g \cdot x} = gG_xg^{-1}$

Proof:

$$\begin{aligned} g' \in G_{g\cdot x} &\iff g' \cdot (g \cdot x) = g \cdot x \\ &\iff (g^{-1}g'g) \cdot x = x \iff g^{-1}g'g \in G_x \iff g' \in gG_xg^{-1}. \ \blacksquare \end{aligned}$$

Corollary: Suppose $G \curvearrowright X$ and $|X| < \infty$. Then $g \mapsto |\mathrm{Fix}(g)|$ is a class function, meaning that $|\mathrm{Fix}(g'g(g')^{-1})| = |\mathrm{Fix}(g)|$ (or in other words $|\mathrm{Fix}(g)|$ is constant on any given conjugate classes).

Proof:

$|\mathrm{Fix}(g'g(g')^{-1})| = |g' \cdot \mathrm{Fix}(g)|$ by the last lemma. And since $x \mapsto g' \cdot x$ is an element of S_X, we know that $|g' \cdot \mathrm{Fix}(g)| = |\mathrm{Fix}(g)|$. $\blacksquare$

The G-orbit of $x \in X$ is the set of all points in X that are G-similar to x. Or to put into other words, we define $G \cdot x \coloneqq \{g \cdot x \in X : g \in G\}$ and say that x' is G-similar to x if $x' = g \cdot x \in G \cdot x$ for some $g \in G$. Also, in that case we denote $x' \sim x$.

Lemma: $\sim$ is an equivalence relation.

Proof:

- $x \sim x$ as $1_G \cdot x = x$.
- $x \sim y \implies y \sim x$ as $x = g \cdot y \implies g^{-1} \cdot x = y$.
- If $x \sim y$ and $y \sim z$ then let $g_1, g_2 \in G$ be such that $x = g_1 \cdot y$ and $y = g_2 \cdot z$. Then $x = (g_1g_2) \cdot z$. So $x \sim z$. $\blacksquare$

It's now clear that the G-orbit of x: $G \cdot x$, is the equivalence class of x with respect to $\sim$. Thus, we define $X/G \coloneqq \{G \cdot x : x \in X\}$. Also note that X/G is a partition of X. As a result, we know that $|X| = \sum_{G\cdot x \in X/G} |G \cdot x|$.

Theorem (Orbit-stabilizer): The map $G/G_x \to G \cdot x$ given by $gG_x \mapsto g \cdot x$ is a bijection. Hence $|G \cdot x| = [G : G_x]$ (where the latter is the number of left cosets of G in G_x).

Proof:

We first show this map is well-defined. Suppose $g_1G_x = g_2G_x$. Then $g_2 = g_1h$ for some $g \in G_x$. And in turn $g_2 \cdot x = (g_1h) \cdot x = g_1 \cdot (h \cdot x) = g_1 \cdot x$.

Next we show injectivity. Assume $g_1 \cdot x = g_2 \cdot x$. Then $g_2^{-1} \cdot (g_1 \cdot x) = x$. So $g_2^{-1}g_1 \in G_x$. Or in other words, $g_1G_x = g_2G_x$.

Finally, surjectivity is obvious from the fact that $G \cdot x$ is the set of $y \in X$ such that there exists $g \in G$ with $g \cdot x = y$. $\blacksquare$

Note that $|G \cdot x| = 1$ iff $\forall g \in G,\ \ g \cdot x = x$ iff $x \in \mathrm{Fix}(G)$ where:

$$\mathrm{Fix}(G) = X^G := \{x \in X : \forall g \in G,\ \ g \cdot x = x\}.$$

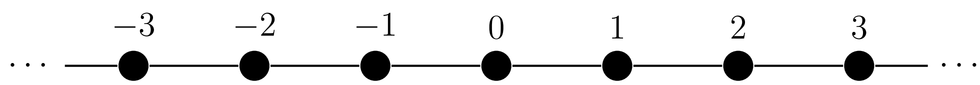
This leads to the equation:

$$|X| = \sum_{\substack{G\cdot x \in X/G \\ |G\cdot x|=1}} |G \cdot x| + \sum_{\substack{G\cdot x \in X/G \\ |G\cdot x|>1}} |G \cdot x| = |\mathrm{Fix}(G)| + \sum_{\substack{G\cdot x \in X/G \\ |G\cdot x|>1}} [G : G_x].$$

I need to do the rest of the math 200a homework still. So I'm going to take a break from taking lecture notes to do the homework.

Set 1 Problem 3: Find the automorphism group of the Cayley graph of $\mathbb{Z}$ with respect to $\{-1, +1\}$.

To start off, note that $\{n, m\}$ is an edge of $\mathrm{Cay}(\mathbb{Z}, \{-1, 1\})$ iff $n - m = \pm 1$. This yields the infinite graph which I've attempted to draw below.



Now from this graph it is clear that reversing the graph is a symmetry. Specifically, define $\tau(n) = -n$. Then $\tau(n) - \tau(m) = -n - (-m) = m - n = -(n - m)$. Hence, $n - m = \pm 1$ iff $\tau(n) - \tau(m) = \mp 1$ and we thus know that τ preserves the edges of our graph and is thus a symmetry.

Another obvious symmetry of our graph are index shifts. Specifically define $\sigma(n) = n + 1$. Then $\tau(n) - \tau(m) = n - m$ for all $n, m \in \mathbb{N}$ and it is thus obvious that τ preserves the edges of graph and is a symmetry.

I glossed over this point before but technically we also need to show σ and τ are bijections. To do this, just note that σ^{-1} is given by $n \mapsto n - 1$ and $\tau^{-1} = \tau$. So, both maps are invertible.

Now we claim that every automorphism of $\mathrm{Cay}(\mathbb{Z}, \{-1, 1\})$ is some composition of τ and σ. To prove this, let θ be any arbitrary automorphism. We know that $\theta(0) = k$ for some $k \in \mathbb{Z}$. And in turn we have that $(\sigma^{-k} \circ \theta)(0) = 0$. Next note that $(\sigma^{-k} \circ \theta)(1)$ equals either $+1$ or -1. In the former case, we can trivially say that $\tau^0 \circ \sigma^{-k} \circ \theta$ fixes both 0 and 1. As for the latter case, since $\tau(0) = 0$ and $\tau(-1) = +1$, we can say that $\tau^1 \circ \sigma^{-k} \circ \theta$ fixes both 0 and 1. Either way, this shows there exists a graph automorphism $\psi = \sigma^k \circ \tau^i$ (where $k \in \{\mathbb{Z}\}$ and $i \in \{0, 1\}$) such that $\psi^{-1} \circ \theta$ fixes both 0 and 1.

Observation: If $\phi \in \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}, \{-1, 1\}))$ with $\phi(0) = 0$ and $\phi(1) = 1$, then $\phi = \mathrm{Id}$.

To prove this, we do induction separately on the positive integers and then on the negative integers.

- Suppose $n \geq 1$ and we've already shown that $\phi(k) = k$ for all $0 \leq k \leq n$. Then since ϕ is a graph automorphism, we must have that $\phi(n + 1) = \phi(n) \pm 1$. But since ϕ is a bijection and we already know that $\phi(n - 1) = n - 1 = \phi(n) - 1$, this means we can only have that $\phi(n + 1) = \phi(n) + 1 = n + 1$. By induction this means that $\phi(n) = n$ for all $n \geq 0$.

- Next suppose $n \leq 0$ and we've shown for all $k \geq n$ that $\phi(k) = k$. Then like before we must have that $\phi(n - 1) = \phi(n) \pm 1 = n \pm 1$ since ϕ is a graph automorphism. But since ϕ is a bijection and we already know $\phi(n+1) = n+1$, we can only have $\phi(n-1) = n-1$. By induction this means that $\phi(n) = n$ for all $n \in \mathbb{Z}$.

Thus $\psi^{-1} \circ \theta = \mathrm{Id}$. Or in other words $\theta = \psi = \sigma^k \tau^i$ where $k \in \mathbb{Z}$ and $i \in \{0, 1\}$. This shows that $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}, \{-1, 1\})) = \langle \sigma, \tau \rangle$.

Now the homework sheet specifically tells us to list out all the elements of the group of automorphisms. To do this, we need to show that $\sigma^{k_1} \circ \tau^{i_1} \neq \sigma^{k_2} \circ \tau^{i_2}$ if either $k_1 \neq k_2$ or $i_1 \neq i_2$.

To start off, note that σ^{k_1} and σ^{k_2} are easily checked to not equal each other when $k_1 \neq k_2$. We merely note that $\sigma^{k_1}(0) = k_1 \neq k_2 = \sigma^{k_2}(0)$.

Also, it is easy to see that $\langle \sigma \rangle = \{\sigma^k : k \in \mathbb{Z}\}$ is a cyclic subgroup of our collection of symmetries and that τ is not in that subgroup. After all the only $k \in \mathbb{Z}$ such that $\sigma^k(0) = \tau(0)$ is $k = 0$. However, $\sigma^0(1) = 1 \neq -1 = \tau(1)$. It now follows that $\langle \sigma \rangle$ and $\langle \sigma \rangle \tau$ are two disjoint cosets which partition our collection of symmetries.

Finally, we need to show that if $k_1 \neq k_2$ then $\sigma^{k_1} \circ \tau \neq \sigma^{k_2} \circ \tau$. To do this, suppose $\sigma^{k_1} \circ \tau = \sigma^{k_2} \circ \tau$. Then by composing τ on the right side we get that $\sigma^{k_1} = \sigma^{k_2}$. And by prior work, we thus know that $k_1 = k_2$.

Thus $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}, \{-1, 1\})) = \{\sigma^k \circ \tau^i : k \in \mathbb{Z} \text{ and } i \in \{0, 1\}\}$ and we know that the representation $\theta = \sigma^k \circ \tau^i$ is unique.

As for showing how to compose elements note that:

$$\tau \circ \sigma \circ \tau(n) = \tau \circ \sigma(-n) = \tau(-n+1) = n - 1 = \sigma^{-1}(n).$$

And since conjugation is a group automorphism, we know that:

- $(\sigma^m \circ \tau) \circ \sigma^n = \sigma^m \circ (\tau \circ \sigma^n \circ \tau) \circ \tau = \sigma^m \circ (\tau \circ \sigma \circ \tau)^n \circ \tau = \sigma^m \circ \sigma^{-n} \circ \tau$
  $= \sigma^{m-n} \circ \tau,$
- $(\sigma^m \circ \tau) \circ (\sigma^n \circ \tau) = \sigma^m \circ (\tau \circ \sigma^n \circ \tau) = \sigma^m \circ (\tau \circ \sigma \circ \tau)^n = \sigma^m \circ \sigma^{-n} = \sigma^{m-n},$
- $\sigma^m \circ (\sigma^n \circ \tau) = \sigma^{m+n} \circ \tau$ and $\sigma^m \circ \sigma^n = \sigma^{m+n}$. ■

Set 1 Problem 2: Suppose G is a finite group and that for every positive integer n:

$$|\{g \in G : g^n = e\}| \leq n$$

(where e is the identity element of G). Use the following steps to prove that G is a cyclic group.

(a) Prove that if there is an element of order d in G, then there are exactly $\phi(d)$ elements of order d in G where $\phi(d)$ is the Euler ϕ-function (where as a reminder $\phi(d)$ equals the number of integers between 1 and d inclusive which are coprime to d).

Suppose $g \in G$ with $o(g) = d$ and then consider the cyclic subgroup $\langle g \rangle \subseteq G$. We know that $o(g^k) = \frac{o(g)}{\gcd(o(g),k)} = \frac{d}{\gcd(d,k)} = d$ iff $\gcd(k, d) = 1$. So by considering g^k for each $k \in \{1, \ldots, d\}$ with $\gcd(d, k) = d$ we get that there are at least $\phi(d)$ distinct elements of G with order d.

That said, all g^k where $k \in \{0, \ldots, d-1\}$ are distinct elements of $\{g \in G : g^d = e\}$. And since $|\{g \in G : g^d = e\}| \leq d$, this proves that $h \in G$ can satisfy that $h^d = e$ only if $h = g^k$ for some integer k. And also because h^d equaling e is a necessary condition for us to have $o(h) = d$, we know that the $\phi(d)$ elements of G we found before are the only elements of G with order d.

(b) For every positive number d, let $\psi(d)$ be the number of elements of G that have order d. Show that $\psi(d) \leq \phi(d)$ and that $\psi(d) \neq 0$ implies that $d \,|\, |G|$.

We know that $\phi(d) \geq 1$ for all positive d since $\gcd(1, d) = 1$. So, if $\psi(d) = 0$, then we trivially know that $\psi(d) \leq \phi(d)$. Meanwhile, if $\psi(d) > 0$ then we showed in part (a) that $\psi(d) = \phi(d)$. Hence in either case we have that $\psi(d) \leq \phi(d)$.

Also, the fact that $d \,|\, |G|$ if $\psi(d) \neq 0$ is just a result of Lagrange's theorem (since the order of any subgroup of G must divides $|G|$ and $\phi(d) \neq 0$ implies there is a cyclic subgroup of G with order d).

(c) Prove that $\psi(d) = \phi(d)$ if d is a positive divisor of $|G|$. Deduce that G is a cyclic group.

Let $n = |G|$ and note that $\sum_{d\,|\,n} \psi(d) = n$ since every element of G has some order dividing n. At the same time, it is a somewhat well known result that $\sum_{d\,|\,n} \phi(d) = n$ for all $n \in \mathbb{N}$.

I can't find a proof of this result anywhere in my notes so I guess I'll prove it here.

Let $S = \{1, \ldots, n\}$ and define $S_d \coloneqq \{k \in S : \gcd(k, n) = d\}$ for each d. Clearly, the S_d form a partition of S as we range over all the divisors of n. Also note that there is a bijective correspondence between S_d and $E_{n/d} \coloneqq \{k \in \{1, \ldots, \frac{n}{d}\} : \gcd(k, \frac{n}{d}) = 1\}$.

Specifically note that $\gcd(m, n) = d \implies \frac{m}{d}, \frac{n}{d} \in \mathbb{Z}$ with $\gcd(\frac{m}{d}, \frac{n}{d}) = 1$. And if we also have that $m \leq n$ then clearly $\frac{m}{d} \leq \frac{n}{d}$. So, $m \in S_d \implies \frac{m}{d} \in E_{n/d}$. Meanwhile, if $\gcd(m, \frac{n}{d}) = 1$, then we know that $\gcd(dm, n) = d$. And also if $m \leq \frac{n}{d}$, then we know that $md \leq n$ Hence $m \in E_{n/d} \implies dm \in S_d$. It now follows that the map $m \mapsto \frac{m}{d}$ is an invertible map from S_d to $E_{n/d}$.

Now $|S_d| = |E_{n/d}| = \phi(\frac{n}{d})$. Also, we know that $n = |S| = \sum_{d\,|\,n} |S_d|$. So we have shown that $n = \sum_{d\,|\,n} \phi(\frac{n}{d}) = \sum_{d\,|\,n} \phi(d)$.

Since $\psi(d) \leq \phi(d)$ for all d, we thus have that:

$$n = \sum_{d\,|\,n} \psi(d) \leq \sum_{d\,|\,n} \phi(d) = n.$$

And this proves that $\sum_{d\,|\,n} \psi(d) = \sum_{d\,|\,n} \phi(d)$. Going even further, since $0 \leq \psi(d) \leq \phi(d)$ for all d, the two sums can only equal if $\psi(d) = \phi(d)$ for all d being summed over. In particular, we must have that $\phi(n) = \psi(n) \geq 1$. So, there is some element of order $n = |G|$ in G. This is equivalent to saying that G is cyclic. ■

Set 1 Problem 1: Suppose G_1 and G_2 are two groups. We say G_1 and G_2 are algebraically independent if there are no proper normal subgroups N_1 and N_2 of G_1 and G_2 respectively such that $G_1/N_1 \cong G_2/N_2$.

(a) Prove that G_1 and G_2 are algebraically independent if and only if $G_1 \times G_2$ satisfies the following property: suppose H is a subgroup of $G_1 \times G_2$ and the projection of H to the i-th component is G_i for $i = 1, 2$. Then $H = G_1 \times G_2$.

As a reminder, the group $G_1 \times G_2$ is just the cartesian product of the two groups equipped with the law of composition that $(g_1, g_2)(g_1', g_2') = (g_1g_1', g_2g_2')$.

$(\Longrightarrow)$
Suppose G_1 and G_2 are algebraically independent and then consider any subgroup $H \subseteq G_1 \times G_2$ such that $\pi_1(H) = G_1$ and $\pi_2(H) = G_2$ (where π_1 and π_2 are the projection maps). Also let e_1 and e_2 denote the identity elements of G_1 and G_2 respectively.

To start off, let $N_1 := H \cap (\{e_1\} \times G_2)$ and $N_2 := H \cap (G_1 \times \{e_2\})$. Then set $N_1' := \pi_2(N_1)$ and $N_2' := \pi_1(N_2)$. Both N_1 and N_2 are easily seen to be subgroups of $G_1 \times G_2$ as they are both intersections of groups. From there it also easy to see that N_1' and N_2' are subgroups of G_2 and G_1 respectively on account of being images of N_2 and N_1 via the homomorphisms π_2 and π_1. And of course there are obvious group isomorphisms showing that $N_1' \cong N_1$ and $N_2' \cong N_2$.

Our first big step is to show that N_1' and N_2' are normal subgroups (which in turn means that G_1/N_2' and G_2/N_1' are well-defined quotient groups).

Suppose $g_1 \in N_2'$ and let g_1' be any element of G. Since $\pi_1(H) = G_1$, we know there is some $g_2' \in G_2$ such that $(g_1', g_2') \in H$. And since H is closed under inverses, we also know that $((g_1')^{-1}, (g_2')^{-1}) \in H$. Therefore $g_1'g(g_1')^{-1} \in N_2'$ since $(g_1'g(g_1')^{-1}, g_2'e_2(g_2')^{-1}) = (g_1'g(g_1')^{-1}, e_2) \in H$. This proves that N_2' is normal in G_1. Analogous reasoning shows that N_1' is normal in G_2.

Next we define a group homomorphism ϕ from G_1 to G_2/N_1' as follows:

Given any $g_1 \in G$, let $\phi(g_1) = g_2N_1'$ where $(g_1, g_2) \in H$.

To show this is well defined, suppose $g_2, g_2' \in G_2$ both satisfy that $(g_1, g_2) \in H$ and $(g_1, g_2') \in H$. Then $(e_1, g_2^{-1}g_2') \in H$, which in turns means that $g_2^{-1}g_2' \in N_1'$. This is equivalent to saying that $g_2^{-1}g_2'N_1' = N_1'$ which in turn is equivalent to saying that $g_2'N_1' = g_2N_1'$.

Also, to see that ϕ is a homomorphism, suppose $(g_1, g_2), (g_1', g_2') \in H$. Then $(g_1g_1', g_2g_2') \in H$ and so $\phi(g_1g_1') = g_2g_2'N_1'$. But we also have that $\phi(g_1)\phi(g_2) = g_2N_1'g_2'N_1' = g_2g_2'N_1'$. So $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$.

Now we claim ϕ is surjective. After all, $\pi_2(H) = G_2$ so for all $g_2 \in G_2$ there exists $g_1 \in G_1$ such that $(g_1, g_2) \in H$. And then in turn $\phi(g_1) = g_2N_1'$. We also claim that the kernel of ϕ is N_2'. After all, suppose $\phi(g_1) = N_1'$. Then we know that there is some $g_2 \in G_2$ such that $(g_1, g_2) \in H$ and $(e_1, g_2) \in H$. But since $(e_1, g_2) \in H$, we also know that $(e_1, g_2^{-1}) \in H$, and thus $(e_1g_1, g_2^{-1}g_2) = (g_1, e_2) \in H$. So, $g_1 \in N_2'$ and we've shown that $\ker(\phi) \subseteq N_2'$. Going the other direction and showing $N_2' \subseteq \ker(\phi)$ is as simple as noting that $e_2N_1' = N_1'$.

By the first isomorphism theorem, we are thus able to conclude that $\frac{G}{N_2'} \cong \frac{G}{N_1'}$.

I ran out of time so everything after this point is not being graded...

Since G_1 and G_2 are algebraically independent, this implies that $N_2' = G_1$ and $N_1' = G_2$. But now since $G_1 \times \{e_2\}$ and $\{e_1\} \times G_2$ are both contained in H are easily seen to together generate all of $G_1 \times G_2$, we know that $H = G_1 \times G_2$. This proves the property in the problem statement.

$(\Longleftarrow)$
Suppose G_1 and G_2 are not algebraically independent and let N_1 and N_2 be proper normal subgroups of G_1 and G_2 such that $G_1/N_1 \cong G_2/N_2$. Then let $\phi : G_1/N_1 \to G_2/N_2$ be a group isomorphism.

We define the set $H := \{(g_1, g_2) \in G_1 \times G_2 : \phi(g_1N_1) = g_2N_2\}$ and claim that this is a subgroup of $G_1 \times G_2$.

- Note that $(e_1, e_2) \in H$ since we must have that $\phi(N_1) = N_2$.
- Suppose $(g_1, g_2) \in H$. Then $\phi(g_1N_1) = g_2N_2$. But note that:
  $$N_2 = \phi(N_1) = \phi(g_1^{-1}g_1N_1) = \phi(g_1^{-1}N_1)\phi(g_1N_1) = \phi(g_1^{-1}N_1)g_2N_2.$$
  Therefore $\phi(g_1^{-1}N_1) = (g_2N_2)^{-1} = g_2^{-1}N_2$ and we've shown that $(g_1, g_2) \in H$.
- Suppose $(g_1, g_2), (g_1', g_2') \in H$. Then we have that $\phi(g_1N_1) = g_2N_2$ and $\phi(g_1'N_1) = g_2'N_2$. And since ϕ is a group homomorphism, we get that:
  $$\phi(g_1g_1'N_1)\phi(g_1N_1)\phi(g_1'N_1) = (g_2N_2)(g_2'N_2) = g_2g_2'N_2.$$
  This shows that $(g_1g_1', g_2g_2') \in H$.

Next observe that $\pi_1(H) = G_1$. After all, for any $g_1 \in G_1$ we can just pick $g_2 \in \phi(g_1N)$ and then we'll know that $(g_1, g_2) \in H$. We also know that $\pi_2(H) = G_2$. After all, since ϕ is surjective, we know that for any $g_2 \in G_2$ there exists a coset $g_1'N_1 \in G_1/N_1$ such that $\phi(g_1'N_1) = g_2N_2$. And now by just choosing any $g_1 \in g_1'N_1$ we get that $(g_1, g_2) \in H$.

That said, $H \neq G_1 \times G_2$. To see this, just pick any $g_1 \in N_1$ and $g_2 \notin N_2$. Then $\phi(g_1N_1) \neq g_2N_2$ and we have that $(g_1, g_2) \notin H$. ■

(b) Suppose G_1 and G_2 are two finite groups and $\gcd(|G_1|, |G_2|) = 1$. Then G_1 and G_2 are algebraically independent.

Let H be any subgroup of $G_1 \times G_2$ such that $\pi_1(H) = G_1$ and $\pi_2(H) = G_2$. Since π_1 and π_2 are group homomorphisms from $G_1 \times G_2$ to G_1 and G_2 respectively, we know that both $|G_1| = |\pi_1(H)|$and $|G_2| = |\pi_2(H)|$ divide $|H|$. Hence, $\mathrm{lcm}(|G_1|, |G_2|)$ divides $|H|$. Meanwhile, we have by Lagrange's theorem that $|H|$ divides $|G_1 \times G_2| = |G_1||G_2|$.

But now because $\gcd(|G_1|, |G_2|) = 1$, we have that $\mathrm{lcm}(|G_1|, |G_2|) = |G_1||G_2|$ So, we must have $|H| = |G_1||G_2|$. And this proves that $H = G_1 \times G_2$.

By part (a), we can now conclude that G_1 and G_2 are algebraically independent. ■