Before getting to the next theorem, I need to learn some more about quotient topologies.

Lemma 1: If $f : X \to Y$ is a continuous map, then $f \times f : X \times X \to Y \times Y$ (given by $f \times f(x_1, x_2) = (f(x_1), f(x_2))$) is a continuous map.

If $\pi_1, \pi_2$ are the natural projection maps from $Y \times Y$ to $Y$, then we have that $f \times f$ is continuous iff $\pi_1 \circ (f \times f)$ and $\pi_2 \circ (f \times f)$ is continuous. But clearly if $U \subseteq Y$ is an open set then $(\pi_1 \circ (f \times f))^{-1} = f^{-1}(U) \times X$ is open in $X \times X$. And a similar statement holds for $\pi_2 \circ (f \times f)$. Hence $f \times f$ is continuous.

Lemma 2: If $p : X \to Y$ is an open continuous map, then $p \times p : X \times X \to Y \times Y$ is also an open continuous map.

We know from the last lemma that $p$ is continuous. Meanwhile, suppose $U \subseteq X \times X$ is open. Then, we know there is a collection $\{V_\alpha \times W_\alpha\}_{\alpha \in A}$ of rectangles in $X \times X$ such that $V_\alpha, W_\alpha$ are open in $X$ and $U = \bigcup_{\alpha \in A}(V_\alpha \times W_\alpha)$. Then in turn:

$$p \times p(U) = p \times p(\bigcup_{\alpha \in A}(V_\alpha \times W_\alpha)) = \bigcup_{\alpha \in A} p \times p(V_\alpha \times W_\alpha) = \bigcup_{\alpha \in A}(p(V_\alpha) \times p(W_\alpha))$$

But since $p$ is open, we know $p(V_\alpha) \times p(W_\alpha)$ is open in $Y \times Y$. So, $p \times p(U)$ is a union of open sets. ■

Corollary 3: If $p : X \to Y$ is an open quotient map then $p \times p : X \times X \to Y \times Y$ is also an open quotient map.

As for why this will be relevant, suppose $G$ is a topological group and $H \lhd G$. Then if we consider the natural projection map $\pi : G \to G/H$ and equip $G/H$ with the quotient topology (so that $\pi$ is a quotient map), then we have that $\pi$ is an open map.

Why?

Suppose $U \subseteq G$ is open. Then $\pi(U)$ is open in $g/H$ if and only if $\pi^{-1}(\pi(U))$ is open in $G$. But note that $\pi^{-1}(\pi(U)) = \{x \in G : \exists y \in U \ s.t. \ x \in yH\} = UH = \bigcup_{h \in H} Uh$. Since each $Uh$ is open (since $G$ is a topological group), we thus have that $\pi^{-1}(\pi(U))$ is open. ■

Theorem 4: Suppose $X, Y, \overline{X}, \overline{Y}$ are topological spaces, $p_1 : X \to \overline{X}$ and $p_2 : Y \to \overline{Y}$ are quotient maps, and $f, \overline{f}$ are functions such that the following diagram commutes:

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle p_1}\downarrow & & \downarrow{\scriptstyle p_2} \\ \overline{X} & \xrightarrow{\overline{f}} & \overline{Y} \end{array}$$

If $f$ is continuous then so is $\overline{f}$.

Proof:

Let $U \subseteq \overline{Y}$ be open. Then $p_1^{-1}(\overline{f}^{-1}(U)) = (p_2 \circ f)^{-1}(U)$ is open since $f$ and $p_2$ are continuous. And since $p_1$ is a quotient map, we thus know that $\overline{f}^{-1}(U)$ is open. This shows that $\overline{f}$ is continuous. ■

Also I'm dumb because this theorem can be simply restated as an application of the universal property of quotient maps.

Corollary 5: Suppose $G$ is a topological group and $H \lhd G$. Then $G/H$ is a topological group when equipped with the quotient topology (induced by the natural projection map $\pi : G \to G/H$).

By lemma 2 and corollary 3, we know that $\pi \times \pi : G \times G \to G/H \times G/H$ is a quotient map. Also, it is easy to verify that the following diagrams commute:

$$\begin{array}{ccc} G \times G & \xrightarrow{(x,y)\mapsto xy} & G \\ \downarrow{\scriptstyle \pi\times\pi} & & \downarrow{\scriptstyle \pi} \\ G/H \times G/H & \xrightarrow{(xH,yH)\mapsto xyH} & G/H \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{x\mapsto x^{-1}} & G \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ G/H & \xrightarrow{xH\mapsto (xH)^{-1}} & G/H \end{array}$$

Therefore, by theorem 4 we know that the group operations on $G/H$ are continuous and so $G/H$ is a topological group. ■

---

Proposition 11.3: Let $G$ be a topological group.

(a) If $G$ is $T_1$, then $G$ is Hausdorff.

Proof:
If $G$ is $T_1$ and $x \neq y \in G$, then we can find an open set $U$ containing $e$ but not containing $xy^{-1}$. And in turn, by *Proposition 11.1(c) and (d)* there is a symmetric neighborhood $V$ of $e$ such that $xy^{-1} \notin VV$.

Now we know $Vx$ and $Vy$ are neighborhoods of $x$ and $y$. Also, we know $Vx \cap Vy = \emptyset$. After all, if this weren't true than there would exist $v_1, v_2 \in V$ with $v_1 x = v_2 y$. And in turn we'd have that $xy^{-1} = v_1^{-1} v_2$. But since $V$ is symmetric and $xy^{-1} \notin VV$, this is a contradiction.

(b) If $G$ is not $T_1$, then let $H$ be the closure of $\{e\}$. Then $H$ is a normal subgroup, and if $G/H$ is given the quotient topology (i.e. $A \subseteq G/H$ is open if and only if $B = \{x \in G : xH \in A\}$ is open), then $G/H$ is a Hausdorff topological group.

Proof:
$H$ is a subgroup by Proposition 11.1(d). Also, to see why $H$ is normal, suppose $H'$ is a conjugate of $H$ with $H' \neq H$. Because the group product is continuous, we know that $H'$ is also closed. And since $e \in H'$, we know that $H' \cap H$ is a closed proper subset of $H$ containing $\{e\}$. But this contradicts that $H$ is the closure of $\{e\}$. Hence, we conclude $H$ is normal.

Now that we know $H$ is a normal subgroup, we can consider the quotient group $G/H$ equipped with the quotient topology. I already proved that $G/H$ is a topological group. Also note that if $\overline{e}$ is the identity of $G/H$ then $\{\overline{e}\}$ is closed in $G/H$. (This is just a result of the definition of a quotient topology plus the fact that $H$ is closed). In turn, we can see that every singleton in $G/H$ is closed. So, $G/H$ is $T_1$. And by part (a) we have that $G/H$ is Hausdorff. ■

The prior theorem shows that it is not much of a restriction to assume our topological groups are Hausdorff. Hence, we now define that $G$ is a locally compact group if $G$ is an LCH topological group.

Suppose $G$ is a locally compact group. Then a Borel measure $\mu$ on $G$ is called left invariant (or right invariant) if $\mu(xE) = \mu(E)$ (or $\mu(Ex) = \mu(E)$) for all $x \in G$ and $E \in \mathcal{B}_G$. Similarly, a linear functional $I$ on $C_c(G)$ is called left- or right-invariant if $I(L_x f) = I(f)$ or $I(R_x f) = I(f)$ for all $f \in C_c(G)$. Finally, a left (or right) Haar measure on $G$ is a nonzero left-invariant (or right-invariant) Radon measure $\mu$ on $G$.

Let $C_c^+ := \{f \in C_c(G) : f \geq 0 \text{ and } \|f\|_u > 0\}$.

Proposition 11.4: Let $G$ be a locally compact group.

(a) A Radon measure $\mu$ on $G$ is a left Haar measure iff the measure $\widetilde{\mu}$ defined by $\widetilde{\mu}(E) = \mu(E^{-1})$ is a right Haar measure.

Proof:
If $\mu$ is a left Haar measure then:

$$\widetilde{\mu}(Ex) = \mu((Ex)^{-1}) = \mu(x^{-1}E^{-1}) = \mu(E^{-1}) = \widetilde{\mu}(E).$$

Meanwhile if $\widetilde{\mu}$ is a right Haar measure then:

$$\mu(xE) = \mu((E^{-1}x^{-1})^{-1}) = \widetilde{\mu}(E^{-1}x^{-1}) = \widetilde{\mu}(E^{-1}) = \mu((E^{-1})^{-1}) = \mu(E).$$

Also as a side note, you can see that $\widetilde{\mu}$ is a well-defined measure since it is merely the pushforward measure of $\mu$ by the inversion map. (Back on page 193 I was calling this the image measure...)

(b) A nonzero Radon measure $\mu$ on $G$ is a left Haar measure iff $\int f \mathrm{d}\mu = \int L_y f \mathrm{d}\mu$ for all $f \in C_c^+$ and $y \in G$.

$(\Longrightarrow)$
If $\mu$ is a left Haar measure then it is obvious that $\int f \mathrm{d}\mu = \int L_y f \mathrm{d}\mu$ whenever $f$ is a simple function. And by the monotone convergence theorem we can extend this to all $f \in C_c^+$.

$(\Longleftarrow)$
Note that $\mathrm{supp}(L_y f) = y \cdot \mathrm{supp}(f)$ for all $y \in G$ and $f \in C_c(G)$.

After all, $L_y f(x) \neq 0$ iff $f(y^{-1}x) \neq 0$. So if $A = \{x : L_y f(x) \neq 0\}$ and $B = \{x : f(x) \neq 0\}$ then $x \in A$ iff $y^{-1}x \in B$ and that happens iff $x \in yB$. And finally, since translation by $y$ is a homeomorphism on $G$, we have that:

$$\mathrm{supp}(L_y f) = \overline{A} = \overline{yB} = y\overline{B} = y \cdot \mathrm{supp}(f).$$

Thus, for any open set $U \subseteq G$ we know that if $f \in C_c(G)$ with $\mathrm{supp}(f) \subseteq U$ then $L_y f \in C_c(G)$ with $\mathrm{supp}(L_y f) \subseteq yU$. Similarly, if $f \in C_c(G)$ with $\mathrm{supp}(f) \subseteq yU$ then $L_{y^{-1}} f \in C_c(G)$ with $\mathrm{supp}(L_{y^{-1}} f) \subseteq U$. And when you consider for all open sets $V \subseteq G$ that $\mu(V) = \sup\{\int f \mathrm{d}\mu : f \in C_c(G), 0 \leq f \leq 1, \mathrm{supp}(f) \subseteq V\}$, it becomes clear that $\mu(yU) = \mu(U)$ for all $y \in G$ and open sets $U \subseteq G$.

As for the case that $E$ is a general Borel subset of $G$, we can just approximate $E$ and $xE$ using open sets.

(c) If $\mu$ is a left Haar measure on $G$, then $\mu(U) > 0$ for every nonempty open $U \subseteq G$ and $\int f \mathrm{d}\mu > 0$ for all $f \in C_c^+$.

Proof:
Since $\mu \neq 0$, we can show by the regularity properties of $\mu$ that there exists a compact set $K \subseteq G$ with $\mu(K) > 0$. Then, for any open nonempty set $U \subseteq G$ we have that $K$ can be covered by finitely many left translates of $U$. Hence, $\mu(U) > 0$.

Next, if $f \in C_c^+$ then let $U := \{x : f(x) > \frac{1}{2}\|f\|_u\}$. $U$ is open since $f$ is continuous. Therefore, since $\mu(U) > 0$ we have that $\int f \mathrm{d}\mu \geq \frac{1}{2}\|f\|_u \mu(U) > 0$.

(d) If $\mu$ is a left Haar measure on $G$ then $\mu(G) < \infty$ iff $G$ is compact.

Proof:
The $(\Longleftarrow)$ direction is obvious from the definition of a Radon measure. Meanwhile, suppose $G$ is not compact and let $V$ be a compact neighborhood of $e$. Then we know that $G$ cannot be covered by finitely many translates of $V$ (lest $G$ be a finite union of compact sets). So, we may find a sequence $\{x_n\}_{n\in\mathbb{N}}$ such that $x_n \in \bigcup_{j=1}^{n-1} x_j V$ for all $n$.

Next, by proposition 11.1 we can find a symmetric neighborhood $U$ of $e$ with $UU \subseteq V$. Importantly, if $m > n$ and $x_n U \cap x_m U \neq \emptyset$ then we would have that $x_m \in x_n UU \subseteq x_n V$. But that contradicts how we picked our $x_n$. Hence, we know $\{x_n U\}_{n\in\mathbb{N}}$ is a disjoint sequence of sets. And since $\mu(x_n U) = \mu(U) > 0$, we know that $\mu(G) \geq \mu(\bigcup_{n\in\mathbb{N}} x_n U) = \sum_{n\in\mathbb{N}} \mu(x_n U) = \infty$. ■

I'll continue with actually constructing a Haar measure later on *page* ___.

---

**Math 200a Notes:**

If $\sigma \in S_n$ we define $\mathrm{supp}(\sigma) := \{i \in \{1,\dots,n\} : \sigma(i) \neq i\}$. Note that if we consider the obvious injection $S_n \hookrightarrow S_{n+1} \hookrightarrow \cdots$ then $\mathrm{supp}(\sigma)$ doesn't change. Also, we let $\mathrm{Fix}(\sigma) = \{1,\dots,n\} - \mathrm{supp}(\sigma)$.

Note that this definition of $\mathrm{Fix}(\sigma)$ is equivalent to the set of fixed points of $\sigma$ with respect to the obvious group action $S_n \curvearrowright \{1,\dots,n\}$.

We say $\sigma_1, \sigma_2 \in S_n$ are disjoint if $\mathrm{supp}(\sigma_1) \cap \mathrm{supp}(\sigma_2) = \emptyset$.

Lemma: If $\sigma_1, \sigma_2$ are disjoint then $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$ and $o(\sigma_1 \circ \sigma_2) = \mathrm{lcm}(o(\sigma_1), o(\sigma_2))$.

Proof:
For all $i \in \{1,\dots,n\}$, if $i \in \mathrm{Fix}(\sigma) \cap \mathrm{Fix}(\sigma_2)$ then $\sigma_1 \circ \sigma_2(i) = i = \sigma_2 \circ \sigma_1(i)$.

Meanwhile, if $i \in \mathrm{Fix}(\sigma_1)$ and $i \notin \mathrm{Fix}(\sigma_2)$, then $\sigma_2 \circ \sigma_1(i) = \sigma_2(i)$. But now note that:

$$\begin{aligned} i \notin \mathrm{Fix}(\sigma_2) &\implies i \in \mathrm{supp}(\sigma_2) \implies \sigma_2(i) \in \mathrm{supp}(\sigma_2) \\ &\implies \sigma_2(i) \notin \mathrm{supp}(\sigma_1) \\ &\implies \sigma_2(i) \in \mathrm{Fix}(\sigma_1) \implies \sigma_1(\sigma_2(i)) = \sigma_2(i). \end{aligned}$$

So, $\sigma_1 \circ \sigma_2(i) = \sigma_2 \circ \sigma_1(i)$.

The case where $i \notin \mathrm{Fix}(\sigma_1)$ and $i \in \mathrm{Fix}(\sigma_2)$ is similar. And since $\sigma_1$ and $\sigma_2$ are disjoint, we never have the fourth case. This proves $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.

Next, let $o(\sigma_i) = d_i$ for both $i$ and let $\ell = \mathrm{lcm}(d_1, d_2)$. Then we know from before that $(\sigma_1 \circ \sigma_2)^\ell = \sigma_1^\ell \sigma_2^\ell = \mathrm{Id}$. Hence, we must have that $o(\sigma_1\sigma_2)$ divides $\ell$. On the other hand, suppose $(\sigma_1 \circ \sigma_2)^k = 1$. Then by considering the obvious action $\langle \sigma_2 \rangle \curvearrowright \{1, \ldots, n\}$, we know for all $j \in \mathrm{supp}(\sigma_2)$ that $\langle \sigma_2 \rangle \cdot j \subseteq \mathrm{supp}(\sigma_2)$ and in turn $\langle \sigma_2 \rangle \cdot j \subseteq \mathrm{Fix}(\sigma_1)$. It follows that $j = \sigma_1^k \circ \sigma_2^k(j) = \sigma_2^k(j)$ for all $j \in \mathrm{supp}(\sigma_2)$. Hence $\sigma_2^k = \mathrm{Id}$ and we've shown that $d_2 \mid k$.

By analogous reasoning we can show that $d_1 \mid k$. So, $\ell \mid k$. ■

For the sake of convenience I'm just going to refer to $\sigma_2 \circ \sigma_1$ as $\sigma_2\sigma_1$ from now on.

If $k \geq 2$, we say $\sigma \in S_n$ is a $k$-cycle if there are distinct elements $a_1, \ldots, a_k \in \{1, \ldots, n\}$ such that $\mathrm{supp}(\sigma) = \{a_1, \ldots, a_k\}$, $\sigma(a_i) = \sigma(a_{i+1})$ for $i < k$, and $\sigma(a_k) = a_1$. We typically denote a $k$-cycle as $(a_1 \ a_2 \ \cdots \ a_k)$.

A one-cycle is trivial since it is just the identity permutation. So we typically don't count them as "cycles".

Theorem: For all $\sigma \in S_n$ there are disjoint nontrivial cycles $\sigma_1, \ldots, \sigma_m$ such that $\sigma = \sigma_1 \cdots \sigma_m$. Also, this decomposition is unique up to permuting the terms. We call this decomposition a cycle decomposition of $\sigma$.

Proof:

Given any permutation $\sigma \in S_n$, we can say that $\langle \sigma \rangle \curvearrowright \{1, \ldots, n\}$ via the action $\sigma \cdot i = \sigma(i)$. Using this fact we can easily show the existence of a cycle decomposition of $\sigma$.

Given any $a \in \{1, \ldots, n\}$ we know there is a unique smallest integer $k$ such that $\sigma^k(a) = a$. So, define $\sigma_{(a)} = (a \ \sigma(a) \ \sigma^2(a) \ \cdots \ \sigma^{k-1}(a))$. By doing this for all $a \in \{1, \ldots, n\}$, we can see that $\mathrm{supp}(\sigma_{(a)}) = \langle \sigma \rangle \cdot a$ (if $a$ has a non-singleton orbit). Also, it is easy to see that $\mathrm{supp}(\sigma_{(a)}) = \mathrm{supp}(\sigma_{(b)})$ implies that $\sigma_{(a)} = \sigma_{(b)}$. Hence $\Sigma := \{\sigma_{(a)} : a \in \{1, \ldots, n\} \text{ and } \sigma(a) \neq a\}$ is a collection of disjoint cycles. And it is easy to see to that $\sigma$ equals the product of the elements of $\Sigma$ in any order.

As for proving the uniqueness of this cycle decomposition, note that if $\sigma = \tau_1\tau_2 \cdots \tau_\ell$ where each $\tau_i$ is a disjoint cycle, then $a' \in \mathrm{supp}(\tau_i)$ implies that $\tau_i = \sigma_{(a')}$ from before.

To see this, first note that if $a' \in \mathrm{supp}(\tau_i)$ then we can show from the disjointness of the $\tau_i$ that $\sigma^k(a') = \tau_i^k(a')$ for all integers $k$. But then this alligns with how we defined the permutation $\sigma_{(a')} \in \Sigma$.

This says that each $\tau_i$ is equal to some $\sigma_{(a)} \in \Sigma$. Because each of the $\tau_i$ is disjoint, we know this correspondance is injective. Also, it's surjective since otherwise the products of the $\tau_i$ and the $\sigma_{(a)}$ wouldn't be the common permutation $\sigma$. ■

I realize I handwaved this entire proof. But at least I thought about it and wrote down something. Professor Alireza meanwhile skipped proving this.

The cycle type of $\sigma$ is $(\ell_1 \geq \ell_2 \geq \cdots \geq \ell_m)$ where $\{\ell_1, \ldots, \ell_m\}$ is the set of sizes of the orbits of $\langle\sigma\rangle \curvearrowright \{1, \ldots, n\}$.

Lemma: $o(\sigma) = \operatorname{lcm}(\ell_1, \ldots, \ell_m)$ where $(\ell_1 \geq \cdots \geq \ell_m)$ is the cycle type of $\sigma$.

Proof:
Take a cycle decomposition of $\sigma$ and then inductively apply the lemma at the beginning of this section.

Lemma: Let $a_1, \ldots, a_m, a_{m+1}, \ldots, a_{m+n}$ be distinct elements.

(a) $(a_1 \ \cdots \ a_m)(a_m \ \cdots \ a_{m+n}) = (a_1 \ \cdots \ a_{m+n})$.

(b) For any $\sigma \in S_n$, $\sigma(a_1 \ a_2 \ \cdots \ a_m)\sigma^{-1} = (\sigma(a_1) \ \sigma(a_2) \ \cdots \ \sigma(a_m))$.

Proof:
Showing part (a) is as simple as just going through and showing the permutations on either side of the identity map things to the same places.

To show part (b), recall from *page 257* that $\operatorname{Fix}(\sigma\tau\sigma^{-1}) = \sigma \cdot \operatorname{Fix}(\tau)$. (where $A \subseteq \{1, \ldots, n\}$ implies that $\sigma \cdot A \coloneqq \{\sigma(a) : a \in A\}$). In turn:

$$\operatorname{supp}(\sigma\tau\sigma^{-1}) = \sigma \cdot \operatorname{supp}(\tau)$$

And in particular, $\operatorname{supp}(\sigma(a_1 \ \cdots \ a_m)\sigma^{-1}) = \{\sigma(a_1), \ldots, \sigma(a_m)\}$. So we know that the permutations on both sides of our proposed equation have the same support.

Next note for any $k < m$ that $\sigma(a_1 \ \ldots \ a_m)\sigma^{-1}(\sigma(a_k)) = \sigma(a_{k+1})$ (and similarly plugging in $\sigma(a_m)$ gives $\sigma(a_1)$). So the permutations agree on their supports and thus everywhere. ■

Proposition: $\sigma_1, \sigma_2 \in S_n$ are conjugates if and only if they have the same cycle types.

($\Longrightarrow$)
Suppose $\sigma = \tau_1 \cdots \tau_m$ is a cycle decomposition such that $\tau_i$ has cycle length $\ell_i$ and $\ell_1 \geq \ell_2 \geq \cdots \geq \ell_m$. Then the cycle type of $\sigma_1$ is $(\ell_1 \geq \cdots \geq \ell_m \geq 1 \geq \cdots \geq 1)$ (with $n = \sum_{i=1}^{m} \ell_i$ many 1s at the end). Also, if $\sigma_2 = \sigma\sigma_1\sigma^{-1}$ then:

$$\sigma_2 = \sigma\tau_1 \cdots \tau_m\sigma^{-1} = (\sigma\tau_1\sigma^{-1})(\sigma\tau_2\sigma^{-1}) \cdots (\sigma\tau_m\sigma^{-1})$$

Additionally, it's not hard to see that each $(\sigma\tau_i\sigma^{-1})$ is a disjoint cycle of the same length as $\tau_i$. Hence $(\sigma\tau_1\sigma^{-1})(\sigma\tau_2\sigma^{-1}) \cdots (\sigma\tau_m\sigma^{-1})$ is a cycle decomposition of $\sigma_2$ and the order type of $\sigma_2$ is also $(\ell_1 \geq \cdots \geq \ell_m \geq 1 \cdots \geq 1)$.

($\Longleftarrow$)
Suppose the common cycle type is $(\ell_1 \geq \ell_2 \geq \cdots \geq \ell_m)$. Then there exists $n < m$ and cycle decompositions:

- $\sigma_1 = (a_1^{(1)} \ \cdots \ a_{\ell_1}^{(1)})(a_1^{(2)} \ \cdots \ a_{\ell_2}^{(2)}) \cdots (a_1^{(n)} \ \cdots \ a_{\ell_n}^{(n)})$
- $\sigma_2 = (b_1^{(1)} \ \cdots \ b_{\ell_1}^{(1)})(b_1^{(2)} \ \cdots \ b_{\ell_2}^{(2)}) \cdots (b_1^{(n)} \ \cdots \ b_{\ell_n}^{(n)})$

  (Note all $a_i^{(j)}$ are distinct and similarly all $b_i^{(j)}$ are distinct.)

For every $i$ such that $\ell_i = 1$ we pick a different $a_1^{(i)}$ among the fixed points of $\sigma_1$. Similarly, we pick a different $b_1^{(i)}$ among the fixed points of $\sigma_2$ for each $i$ with $\ell_i = 1$. Then finally, we define the permutation $\tau \in S_n$ by $\tau(a_j^{(i)}) = b_j^{(i)}$. Then:

$$\begin{aligned}\tau\sigma_1\tau^{-1} &= (\tau(a_1^{(1)}) \ \cdots \ \tau(a_{\ell_1}^{(1)})) \cdots (\tau(a_1^{(m)}) \ \cdots \ \tau(a_{\ell_m}^{(m)})) \\ &= (b_1^{(1)} \ \cdots \ b_{\ell_1}^{(1)}) \cdots (b_1^{(m)} \ \cdots \ b_{\ell_m}^{(m)}) = \sigma_2. \ \blacksquare\end{aligned}$$

Corollary: The number of conjugate classes of $S_n$ is equal to the number of integer partitions of $n$ (see my paper math 188 notes).

---

By noting that $(a_1 \ a_2 \ \cdots \ a_n) = (a_1 \ a_2)(a_2 \ a_3) \cdots (a_{n-1} \ a_n)$ we can see that every permutation can be written as a product of transpositions (i.e. 2-cycles). That said, except in trivial cases there are many different ways to write a permutation as a product of transpositions. For example, $(1 \ 2)(2 \ 3)(1 \ 2) = (1 \ 3)$. So, is it still possible to characterize permutations somehow by how they are expressed as products of transpositions?

Note that $S_n \curvearrowright \mathbb{Z}[x_1, \ldots, x_n]$ by $(\sigma \cdot f)(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. Also, this group action importantly has the properties that $\sigma \cdot (f + g) = (\sigma \cdot f) + (\sigma \cdot g)$ and $\sigma \cdot (fg) = (\sigma \cdot f)(\sigma \cdot g)$.

If we let $\Delta(x_1, \ldots, x_n) \coloneqq \prod_{i<j}(x_i - x_j)$, then we we have that

$$\Delta^2(x_1, \ldots, x_n) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j}(x_i - x_j).$$

Hence, $(\sigma \cdot \Delta^2) = \Delta^2$ for all $\sigma \in S_n$ (i.e. $\Delta^2$ is a symmetric polynomial). And since $(\sigma \cdot \Delta)^2 = (\sigma \cdot \Delta^2) = \Delta^2$, we must have that $\sigma \cdot \Delta = \pm\Delta$ for each $\sigma \in S_n$. So, there exists a map $\varepsilon : S_n \to \{-1, 1\}$ such that $\sigma \cdot \Delta = \varepsilon(\sigma)\Delta$.

Note that $\sigma \cdot (\sigma' \cdot \Delta) = (\sigma\sigma') \cdot \Delta = \varepsilon(\sigma\sigma')\Delta$. But we also have that:

$$\sigma \cdot (\sigma' \cdot \Delta) = \sigma \cdot (\varepsilon(\sigma')\Delta) = \varepsilon(\sigma')(\sigma \cdot \Delta) = \varepsilon(\sigma')\varepsilon(\sigma)\Delta.$$

Therefore $\varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$. And when you also consider that $\varepsilon(\mathrm{Id}) = +1$, this proves that $\varepsilon$ is a group homomorphism.

One more note is that if $\tau$ is a transposition then $\varepsilon(\tau) = -1$. To see this, just note that if $\tau = (i \ j)$ where $i < j$, then $\tau \cdot \Delta = (-1)^{2(j-i-1)+1}\Delta = -\Delta$.

Thus, if $\sigma \in S_n$ is decomposed into a product of transpositions, we must have that the number of transpositions in that product is even if $\varepsilon(\sigma) = +1$ and odd if $\varepsilon(\sigma) = -1$. In other words, even and odd permutations are well-defined.

We define $A_n \coloneqq \ker(\varepsilon) = \{\text{all even permutations of } S_n\}$. Note that $A_n \lhd S_n$ (since it is a kernel of a group homomorphism).

Theorem: If $n \geq 2$ then $[S_n : A_n] = 2$.

Proof:

By the first isomorphism theorem we have that:

$$S_n/A_n = S_n/\ker(\varepsilon) \cong \operatorname{im}(\varepsilon) = \{-1, +1\}.$$

Hence $[S_n : A_n] = 2$. ■

---

The last theorem that can be tested on the midterm tomorrow is that $A_n$ is a simple group (if $n \geq 5$). So I'll try to prove this and then do some exercises.

Lemma: $A_n$ is generated by the set of 3-cycles.

Proof:

It is enough to show that the product of 2 transpositions is in the subgroup generated by 3 cycles. Fortunately, if $a, b, c, d$ are distinct elements in $\{1, \ldots, n\}$ then:

- $(a\ b)(a\ b) = \mathrm{Id}$
- $(a\ b)(b\ c) = (a\ b\ c)$
- $(a\ b)(c\ d) = (a\ b)(b\ c)(b\ c)(c\ d) = (a\ b\ c)(b\ c\ d)$. ■

Lemma: If $N \lhd A_n$ and $N$ has a 3-cycle then $N = A_n$.

Proof:

Suppose $(a_1\ a_2\ a_3) \in N$. Then for any distinct $b_1, b_2, b_3 \in \{1, \ldots, n\}$ let $\sigma \in S_n$ be a permutation such that $\sigma(a_1) = b_1$, $\sigma(a_2) = b_2$, and $\sigma(a_3) = b_3$. Since $N$ is normal, we have that $(b_1\ b_2\ b_3) = \sigma(a_1\ a_2\ a_3)\sigma^{-1} \in N$. So, $N$ contains all 3-cycles. And by the last lemma this means that $A_n < N$. ■

Theorem: If $n \geq 5$ then $A_n$ is simple.

Proof:

We shall first show that $A_5$ is simple. Note that $|A_5| = \frac{5!}{2} = 60 = 5 \cdot 2^2 \cdot 3$. So suppose for the sake of contradiction that there exists a subgroup $N \lhd A_5$ with $1 \lneqq N \lneqq A_5$.

We can't have that 3 divides $|N|$.

If 3 divides $|N|$ then we would know by Cauchy's theorem that $N$ contains an element of order 3, say $\sigma$. So, let $(\ell_1 \geq \cdots \geq \ell_m)$ be the cycle type of $\sigma$. We must have that $\ell_1 + \ldots + \ell_m = 5$ and $\operatorname{lcm}(\ell_1, \ldots, \ell_m) = 3$. But the only cycle type satisfying those requirements is $(3 \geq 1 \geq 1)$. Hence, $\sigma$ is a 3-cycle. That in turn implies by the last lemma that $N = A_n$ (which is a contradiction).

Similarly, we can't have that 5 divides $|N|$.

Let $P \in \mathrm{Syl}_5(N)$. If $5$ divides $N$ then we also have that $P \in \mathrm{Syl}_5(A_5)$. And since there exists $x \in A_5$ such that $P' = xPx^{-1} \subseteq N$ for all $P' \in \mathrm{Syl}_p(A_5)$, we can in turn say that $N$ contains every element of $A_n$ with order dividing $5$.

But now note that the only elements of $S_5$ with order $5$ are $5$ cycles. Also, all $5$ cycles are easily seen to be even permutations. So, $\{\sigma \in S_5 : \sigma \text{ is a } 5\text{-cycle}\}$ is a subset of $N$. Also, it is an easy counting exercise to see that the number of such permutations is $^{5!}/_5 = 24$. Hence, we've proven that $24 < |N|$.

Since $|N|$ divides $60$ and $N \lneq A_5$, this forces $|N| = 30$. But we already showed that $3$ can't divide $|N|$. So, we have a contradiction.

This narrows us down to the case that $|N| = 2$ or $|N| = 4$. To address this case, we bring up the following lemma:

Lemma: If $|G| < \infty$, $N \lhd G$, and $N$ is a $p$-group, then $N \subseteq \bigcap_{P \in \mathrm{Syl}_p(G)} P =: O_p(G)$.

Proof:
By Sylow's 2nd theorem we know $N \subseteq P_0$ for some $P_0 \in \mathrm{Syl}_p(G)$. Then since $N$ is normal, $N = \bigcap_{x \in G} xNx^{-1} \subseteq \bigcap_{x \in G} xP_0x^{-1} = \bigcap_{P \in \mathrm{Syl}_p(G)} P$. ■

Now pick $\sigma \in A_5$ with $o(\sigma) = 2$. The only cycle types of permutations in $S_5$ that yield permutations of order $2$ are $(2 \geq 1 \geq 1 \geq 1)$ and $(2 \geq 2 \geq 1)$. However, permutations of the former cycle type are odd. Hence, we may assume $\sigma = (a\ \ b)(c\ \ d)$.

Next, note that $P_2 := \{\mathrm{Id}, (1\ \ 2)(3\ \ 4), (1\ \ 3)(2\ \ 4), (1\ \ 4)(2\ \ 3)\}$ is a Sylow $2$-subgroup of $A_5$.

It is clear that $P_2$ is closed under inverses. We only need to verify that it really is closed under compositions.

- $(1\ \ 2)(3\ \ 4)(1\ \ 3)(2\ \ 4) = (1\ \ 4)(2\ \ 3)$ and $(1\ \ 2)(3\ \ 4)(1\ \ 4)(2\ \ 3) = (1\ \ 3)(2\ \ 4)$,
- $(1\ \ 3)(2\ \ 4)(1\ \ 2)(3\ \ 4) = (1\ \ 4)(2\ \ 3)$ and $(1\ \ 3)(2\ \ 4)(1\ \ 4)(2\ \ 3) = (1\ \ 2)(3\ \ 4)$,
- I'm bored and don't want to manually verify the last two relations.

Thus by our lemma, we know that $N \subseteq \bigcap_{P \in \mathrm{Syl}_2(G)} P = \bigcap_{x \in G} xP_2x^{-1}$.

But now note that:

$$((a\ \ b)(c\ \ e))P_2((a\ \ b)(c\ \ e))^{-1} = \{\mathrm{Id}, (b\ \ a)(e\ \ d), (b\ \ e)(a\ \ d), (b\ \ d)(a\ \ e)\}$$

Therefore $\bigcap_{x \in G} xP_2x^{-1}$ is trivial and we have a contradiction since $N = \{\mathrm{Id}\}$. This finishes the proof that $A_5$ is simple.

---

Now we proceed by induction on $n$. Suppose $1 \neq N \lhd A_n$ and for all $i \in \{1, \ldots, n\}$ let $G_i := \{\sigma \in A_n : \sigma(i) = i\}$. Then there is an obvious group isomorphism such that $G_i \cong A_{n-1}$ for all $i$. Also, $N \cap G_i \lhd G_i$. So, by induction we know for each $i$ that either $N \cap G_i = \{1\}$ or $N \cap G_i = G_i$.

But if $N \cap G_i = G_i$ for any $i$ then we are already done since that would imply that $N$ contains a 3-cycle. So, without loss of generality we may now assume that $N \cap G_i = \{\mathrm{Id}\}$ for all $i$. As a consequence, if $\sigma, \sigma' \in N$ satisfy that $\sigma(i) = \sigma'(i)$ for any $i$ then we must have that $\sigma = \sigma'$ since $\sigma(\sigma')^{-1} \in N \cap G_i$.

Suppose $\sigma \in N - \{\mathrm{Id}\}$. Then we have two cases:

- Suppose $\sigma$ has a cycle of size $\geq 3$. In other words, there exists distinct numbers $a, b, c \in \{1, \ldots, n\}$ such that $\sigma = (a\ b\ c\ \cdots)\cdots$. But now if $d, e \in \{1, \ldots, n\}$ are any other 2 distinct numbers, we have that $\sigma' := (c\ d\ e)\sigma(c\ d\ e)^{-1} \in N$ with $\sigma'(a) = b = \sigma(a)$ and $\sigma'(b) = d \neq c = \sigma(b)$. This is a contradiction.
- Meanwhile, suppose $\sigma$ has only cycles of length 2. Since $\sigma$ is even, we thus know there are distinct numbers $a, b, c, d \in \{1, \ldots, n\}$ such that $\sigma = (a\ b)(c\ d)\cdots$. But now if $e, f$ are two other distinct elements of $\{1, \ldots, n\}$ (supposing $n \geq 6$), then consider $\sigma' := (c\ e\ f)\sigma(c\ e\ f)^{-1}$. Like before, $\sigma'(a) = b = \sigma(a)$. But $\sigma'(d) = e \neq c = \sigma(d)$. Hence we again have a contradiction. ■

---

Here is an application of the prior theorem. Suppose $G$ is a finite group with $|G| = 2m$ where $2 \nmid m$. Then there exists a characteristic subgroup $N < G$ such that $[G : N] = 2$.

Proof:
Consider the action of $G \curvearrowright G$ by left translations and let $\phi : G \to S_G$ be the induced group homomorphism. Note that we can always identify $S_G$ with $S_{|G|}$ by just numbering the elements of $G$. Also note that for all $g \in G$ the cycle type of $\phi(g)$ is:
$(o(g) \geq o(g) \geq \cdots \geq o(g))$ (where there are $|G|/o(g)$ many orbits).

Next, by Cauchy's theorem there exists $g_0 \in G$ such that $o(g_0) = 2$. But now the cycle type of $\phi(g_0)$ is $(2 \geq 2 \geq \cdots \geq 2)$ (with $|G|/2 = m$ many orbits.) Hence, $\phi(g_0)$ is an odd permutation and we know that $\varepsilon \circ \phi : G \to \{\pm 1\}$ is a surjective group homomorphism.

Let $N := \ker(\varepsilon \circ \phi)$. Then $[G : N] = |\mathrm{im}(\varepsilon \circ \phi)| = 2$. Also, because of how we defined $N$ we know that $g \in N$ if and only if the cycle type of $(o(g) \geq o(g) \geq \cdots \geq o(g))$ gives an even permutation.

But now note that for all $\theta \in \mathrm{Aut}(G)$ we have that $o(\theta(g)) = o(g)$. Thus $g \in N$ iff $\theta(g) \in N$ for all $\theta \in \mathrm{Aut}(G)$. And this implies that $N$ is a characteristic subgroup of $G$. ■

---

(I didn't do these problems before they were due but I'm doing them now...)

**Set 4 Problem 5:** In this problem we show that $\mathrm{Inn}(S_6) \neq \mathrm{Aut}(S_6)$.

(a) Show that $S_5$ has 6 Sylow 5-subgroups and then use the action of $S_5$ on $\mathrm{Syl}_5(S_5)$ to show that $S_6$ has a subgroup $H$ which is isomorphic to $S_5$.

Since $s_5 := |\mathrm{Syl}_5(S_5)|$ equals $1 \pmod 5$ and divides $\frac{|S_5|}{5} = \frac{5!}{5} = 24$, that already restricts $s_5$ to equaling either 1 or 6. That said, as I will prove later on *page* ___ in my lecture notes, $S_5$ does not have a normal subgroup of size 5. Therefore, this forces $s_5 = 6$.

Now consider the action $S_5 \curvearrowright \mathrm{Syl}_5(S_5)$ by conjugation and let:

$$\phi : S_5 \to S_{\mathrm{Syl}_5(S_5)} \cong S_6 \text{ be the induced homomorphism.}$$

Note that $\sigma \in \ker(\phi)$ iff $\sigma P \sigma^{-1} = P$ for all $P \in \mathrm{Syl}_5(G)$. In particular, if we fix $P \in \mathrm{Syl}_5(G)$ then we know that $\ker(\phi) \subseteq N_G(P)$ and hence:

$$|\ker(\phi)| \leq \tfrac{S_5!}{s_5} = \tfrac{120}{6} = 20.$$

Thus $\ker(\phi) \lhd S_5$ and $[S_5 : \ker(\phi)] > 2$. By the aforementioned proof on ***page*** ___, this means that $\ker(\phi) = \{\mathrm{Id}\}$. Hence $\phi$ is an injective homomorphism. And by letting $H := \mathrm{im}(\phi)$ we have that $S_5 \cong H < S_6$.

(b) Show for every $\sigma \in S_6$ that $\mathrm{Fix}(\sigma H \sigma^{-1}) = \emptyset$ (where $S_6$ is acting on $\{1, \ldots, 6\}$ by evaluation).

We know that $\mathrm{Fix}(\sigma H \sigma^{-1}) = \bigcap_{\tau \in H} \mathrm{Fix}(\sigma \tau \sigma^{-1}) = \bigcap_{\tau \in H} (\sigma \cdot \mathrm{Fix}(\tau))$. But now recall that the action $S_5 \curvearrowright \mathrm{Syl}_5(S_5)$ is transitive and hence there is some $\tau' \in H$ such that $\mathrm{Fix}(\tau') = \emptyset$. In turn, $\sigma \cdot \mathrm{Fix}(\tau') = \emptyset$ and so $\mathrm{Fix}(\sigma H \sigma^{-1}) = \emptyset$ for all $\sigma \in S_n$.

Another way of thinking of this is that conjugation preserves cycle type. So if $\tau \in S_6$ has no fixed points (i.e. $1$-cycles), then $\sigma \tau \sigma^{-1}$ also has no $1$-cycles.

(c) Consider the action $S_6 \curvearrowright S_6/H$ by left-translation. Show that this induces a group homomorphism $\theta : S_6 \to S_6$ and that $\mathrm{Fix}(\theta(H)) \neq \emptyset$ (again with respect to the action of $S_6$ on $\{1, \ldots, 6\}$ by evaluation).

Since $|H| = |S_5|$, we know $[S_6 : H] = \frac{|S_6|}{|S_5|} = \frac{6!}{5!} = 6$. Hence, by numbering the cosets of $H$ we can say that $S_{S_6/H} \cong S_6$. For convenience, I'll assume the coset $H$ corresponds to $1 \in \{1, \ldots, 6\}$.

Now consider the induced homomorphism $\theta$ described in the problem statement. For any $\tau \in S_6$ we have that $\theta(\tau)$ describes the map $\sigma H \mapsto \tau \sigma H$. But note that if $\tau \in H$ then $\theta(\tau)$ fixes $H$. After applying our correspondance $S_{S_6/H} \cong S_6$ this translates to saying that $1 \in \mathrm{Fix}(\theta(H))$.

(d) Deduce that $\mathrm{Aut}(S_6) \neq \mathrm{Inn}(S_6)$.

In part (b) we proves that if $\psi \in \mathrm{Inn}(S_6)$ then $\mathrm{Fix}(\psi(H)) = \emptyset$. Thus the fact that $\theta$ from part (c) doesn't satisfy that property means $\theta$ is definitely not an inner automorphism. If we can now prove that $\theta$ is in fact an automorphism despite that, then we will be done.

Fortunately, note that $\tau \in \ker(\theta)$ iff $\tau \sigma H = \sigma H$ for all $\sigma \in S_6$. This is equivalent to saying that $\tau \in \bigcap_{\sigma \in S_6} \sigma H \sigma^{-1}$. And in particular, this proves that $\ker(\theta) \subseteq H$. But now since $\ker(\theta) \lhd S_6$ and $[S_6 : \ker(\theta)] > [S_6 : H] > 2$, we know from one more application of the fact on ***page*** ___ that $\ker(\theta) = \{\mathrm{Id}\}$. Hence $\theta$ is injective. And by pigeonhole principle this also proves that $\theta$ is surjective. ■

**Set 4 Problem 6:** Prove that a group $G$ of order $36$ is not simple.

Suppose for the sake of contradiction that $G$ is simple. Then since $s_3 \coloneqq |\mathrm{Syl}_3(G)|$ divides $12$ and equals $1 \pmod 3$, we know $s_3$ must equal either $1$ or $4$. But we can't have that $s_3 = 1$ since that would violate the simplicity of $G$. Hence, we know that $s_3 = 4$.

Next, consider the action $G \curvearrowright \mathrm{Syl}_3(G)$ and let $\phi : G \to S_{\mathrm{Syl}_3(G)} \cong S_4$ be the induced homomorphism. Since that action is transitive, we know that $\ker(\phi) \neq G$. However, we also know that $\ker(\phi) \lhd G$. So by the simplicity of $G$ we must have that $\ker(\phi) = 1$. And this implies by the first isomorphism theorem that there is some subgroup $H = \mathrm{im}(\phi)$ of $S_4$ with $G \cong H$. But this is a contradiction since $|G| = 36 > 24 = |S_4|$. ■

---

# 10/29/2025

Ehh the midterm went mediocrely. I guess I'm one step closer towards flunking out of school. Anyways, right now I want to go back to studying Haar measures. So I'm going to resume what I was doing on *page 353*.

If $G$ is a group and $E, V \subseteq G$, then we can in some sense measure the size of $E$ relative to $V$ by asking what is the minimum cardinality of $A \subseteq G$ such that $E \subseteq \bigcup_{x \in A} xV$. Also, if $E$ is a compact or precompact set and $V$ is open, then we can guarentee that this minimum cardinality is finite.

Clearly, the above construction defines a translation invariant notion of size. But it's not a measure. Can we modify this approach to actually get a measure?

Firstly, we'll switch to working with functions in $C_c^+(G)$ since functions are easier to work with than measures and we can hopefully apply the Riesz representation theorem if we get a positive result when working with functions.

Suppose $f, \phi \in C_c^+(G)$. Then $U = \{x : \phi(x) > \frac{1}{2}\|\phi\|_u\}$ is an open nonempty set. Also, $\mathrm{supp}(f)$ is compact. So there are finitely many $x_1, \ldots, x_n \in G$ with $\mathrm{supp}(f) \subseteq \bigcup_{j=1}^n x_j U$. And we in turn know that:

$$f \leq \tfrac{2\|f\|_u}{\|\phi\|_u} \textstyle\sum_{j=1}^n L_{x_j}\phi.$$

Hence, given any $f, \phi \in C_c^+(G)$ it is well-defined to set:

$$(f : \phi) \coloneqq \inf\left\{\textstyle\sum_{j=1}^n c_j : f \leq \sum_{j=1}^n c_j L_{x_j}\phi \text{ for some } n \in \mathbb{N} \text{ and } x_1, \ldots, x_n \in G\right\}.$$

Note that if $f \leq \sum_{j=1}^n c_j L_{x_j}\phi$ then we have by triangle inequality that $\|f\|_u \leq \|\phi\|_u \sum_{j=1}^n c_j$. Thus, we clearly have that $0 < \frac{\|f\|_u}{\|\phi\|_u} \leq (f : \phi)$.

Lemma 11.5: Suppose that $f, g, \phi \in C_c^+$. Then:

(a) $(f : \phi) = (L_x f : \phi)$ for any $x \in G$.

This is because $f \leq \sum_{j=1}^n c_j L_{x_j}\phi$ iff $L_x f \leq \sum_{j=1}^n c_j L_{xx_j}\phi$.

(b) $(cf:\phi) = c(f:\phi)$ for any $c > 0$.

This is because $f \leq \sum_{j=1}^{n} c_j L_{x_j}\phi$ iff $cf \leq \sum_{j=1}^{n} cc_j L_{x_j}\phi$.

(c) $(f+g,\phi) \leq (f:\phi) + (g:\phi)$.

Suppose $f \leq \sum_{j=1}^{m} c_j L_{x_j}\phi$ and $g \leq \sum_{j=m+1}^{m+n} c_j L_{x_j}\phi$. Then $f+g \leq \sum_{j=1}^{n} c_j L_{x_j}\phi$. And by minimizing $\sum_{j=1}^{m} c_j$ and $\sum_{j=m+1}^{m+n} c_j$ this claim follows.

(d) $(f:\phi) \leq (f:g)(g:\phi)$.

If $f \leq \sum_{j=1}^{n} c_j L_{x_j} g$ and $g \leq \sum_{i=1}^{n} d_i L_{y_i}\phi$, then:

$$f \leq \sum_j c_j L_{x_j}(\sum_{i=1} d_i L_{y_i}\phi) = \sum_j c_j(\sum_i d_i L_{x_j} L_{y_i}\phi) = \sum_{j,i} c_j d_i L_{x_j y_i}\phi$$

And since $\sum_{j,i} c_j d_i = (\sum_j c_j)(\sum_i d_i)$ our claim follows. ■

Now let us fix $f_0 \in C_c^+(G)$ from here on out. It doesn't matter which function $f_0$ specifically is. We just want to have a base-line function to compare all other functions in $C_c^+(G)$ to.

Next, if $\phi \in C_c^+(G)$ then let us define $I_\phi(f) := \frac{(f:\phi)}{(f_0:\phi)}$ for all $f \in C_c^+(G)$.

By the last lemma, we know that $I_\phi$ is a sublinear functional that is invariant to left translations. Also, note that:

$I_\phi(f) = \frac{(f:\phi)}{(f_0:\phi)} \leq \frac{(f:f_0)(f_0:\phi)}{(f_0:\phi)} \leq (f:f_0)$ and $I_\phi(f) = \frac{(f:\phi)}{(f_0:\phi)} \geq \frac{(f:\phi)}{(f_0:f)(f:\phi)} \geq (f_0:f)^{-1}$.

(To put the last line more succinctly, $I_\phi(f) \in [(f_0:f)^{-1}, (f:f_0)]$ for all $f, \phi \in C_c^+(G)$...)

Folland's next claim is that $I_\phi$ is "approximately" linear when $\mathrm{supp}(\phi)$ is small.

Lemma 11.7: If $f_1, f_2 \in C_c^+(G)$ and $\varepsilon > 0$ then there is a neighborhood $V$ of $e \in G$ such that $I_\phi(f_1) + I_\phi(f_2) \leq I_\phi(f_1+f_2) + \varepsilon$ whenever $\mathrm{supp}(\phi) \subseteq V$.

Proof:

Fix $g \in C_c^+$ with $g = 1$ on $\mathrm{supp}(f_1+f_2)$. Then for any $\delta > 0$ define $h_\delta = f_1 + f_2 + \delta g$ and for both $i$ define:

$$h_\delta^{(i)}(x) = \begin{cases} f_i(x)/h_\delta(x) & \text{if } x \in \mathrm{supp}(f) \\ 0 & \text{otherwise.} \end{cases}$$

Then each $h_\delta^{(i)} \in C_c^+(G)$. So by *proposition 11.2* we know there is some neighborhood $V_\delta$ of $e$ with $|h_\delta^{(i)} i(x) - h_\delta^{(i)}(y)| < \delta$ when $y^{-1}x \in V$ and $i \in \{1,2\}$.

Specifically, let $V_\delta$ be a nighborhood of $e$ such that $\|R_z h_\delta^{(i)} - h_\delta^{(i)}\|_u < \delta$ for all $z \in V_\delta$. Then $|h_\delta^{(i)}(x) - h_\delta^{(i)}(y)| < \delta$ if $x = yz$ for some $z \in V_\delta$. Or in other words, if $y^{-1}x = z \in V_\delta$ then $|h_\delta^{(i)}(x) - h_\delta^{(i)}(y)| < \delta$.

If $\phi \in C_c^+(G)$ with $\mathrm{supp}(\phi) \subseteq V_\delta$ and $h_\delta \leq \sum_{j=1}^{n} c_j L_{x_j}\phi$, then $|h_\delta^{(i)}(x) - h_\delta^{(i)}(x_j)| < \delta$ whenever $x_j^{-1}x \in \mathrm{supp}(\phi)$. Hence, we can say for all $x \in G$ that:

$$f_i(x) = h_\delta(x) h_\delta^{(i)} \leq \sum_{j=1}^{n} c_j \phi(x_j^{-1}x) h_\delta^{(i)}(x) \leq \sum_{j=1}^{n} c_j \phi(x_j^{-1}x)(h_\delta^{(i)}(x_j) + \delta)$$

But now this proves that $(f_i : \phi) \leq \sum_{j=1}^{n} c_j(h_\delta^{(i)}(x_j) + \delta)$ for both $i$.

Also, since $h_\delta^{(1)} + h_\delta^{(2)} \leq 1$, we can thus conclude that:
$$(f_1 : \phi) + (f_2 : \phi) \leq \sum_{j=1}^{n} c_j(1 + 2\delta).$$

And by bringing $\sum_{j=1}^{n} c_j$ arbitrarily close to $(h : \phi)$ and dividing by $(f_0 : \phi)$, we can now say that $I_\phi(f_1) + I_\phi(f_2) \leq (1 + 2\delta)I_\phi(h_\delta) \leq (1 + 2\delta)(I_\phi(f_1 + f_2) + \delta I_\phi(g))$.

Now we want $(1+2\delta)(I_\phi(f_1+f_2)+\delta I_\phi(g)) < I_\phi(f_1+f_2)+\varepsilon$. Equivalently this means we want $2\delta I_\phi(f_1+f_2)+\delta(1+2\delta)I_\phi(g) < \varepsilon$. And fortunately, this will be guarenteed if:
$$2\delta(f_1 + f_2 : f_0) + \delta(1 + 2\delta)(g : f_0) < \varepsilon$$

So, by choosing $\delta$ small enough we can guarentee that $I_\phi(f_1) + I_\phi(f_2) \leq I_\phi(f_1 + f_2)$ whenever $\text{supp}(\phi) \subseteq V_\delta$. ■

Theorem 11.8: Every locally compact group $G$ contains a left Haar measure.

Proof:
For each $f \in C_C^+(G)$ let $X_f := [(f_0 : f)^{-1}, (f : f_0)]$. Then let $X = \prod_{f \in C_c^+(G)} X_f$. By Tychonoff's theorem we know that $X$ is a compact Hausdorff space. Also, we have that $I_\phi \in X$ for all $\phi \in C_c^+(G)$ since $I_\phi(f) \in [(f_0 : f)^{-1}, (f : f_0)]$ for all $f, \phi \in C_c^+(G)$.

Now for each neighborhood $V$ of $e$ let $K(V)$ be the closure in $X$ of $\{I_\phi : \text{supp}(\phi) \subseteq V\}$. Then note that $\bigcap_{j=1}^{n} K(V_j) \supseteq K(\bigcap_{j=1}^{n} V_j) \neq \emptyset$ for all finite collections $\{V_1, \ldots, V_n\}$ of neighborhoods of $e$. Hence since $X$ is compact and the collection of sets $K(V)$ has the finite intersection property, we know there exists an element $I$ in the intersection of all the $K(V)$'s.

Next since $I$ is either an accumulation point of or inside $\{I_\phi : \text{supp}(\phi) \subseteq V\}$ for all neighborhoods $V$ of $e$, we know that any neighborhood of $I$ in $X$ must intersect $\{I_\phi : \text{supp}(\phi) \subseteq V\}$ for all neighborhoods $V$ of $e$ in $G$. Consequently, for any neighborhood $V$ of $e$ and any $f_1, \ldots, f_n \in C_c^+(G)$ and $\varepsilon > 0$ there exists $\phi \in C_c^+(G)$ with $\text{supp}(\phi) \subseteq V$ such that $|I(f_j) - I_\phi(f_j)| < \varepsilon$ for each $j$.

Why?
By definition of the product topology, the following is an open neighborhood of $I$ in $X$:
$$U := \{I' \in X : |I(f_j) - I'(f_j)| < \varepsilon \text{ for } j = 1, \ldots, n\}$$

Then any $I_\phi \in U \cap \{I_\phi : \text{supp}(\phi) \subseteq V\}$ satisfies that $|I(f_j) - I_\phi(f_j)| < \varepsilon$ for each $j \in \{1, \ldots, n\}$.

Consequently, we can now show using lemmas 11.5 and 11.7 that $I$ is left-invariant and satisfies that $I(af + bg) = aI(f) + bI(g)$ for all $f, g \in C_c^+$ and $a, b > 0$.

To show that $I(af + bg) = aI(f) + bI(g)$, consider any $\varepsilon > 0$ and then pick a neighborhood $V$ of $e$ such that whenever $\text{supp}(\phi) \subseteq V$ we have that:
$$I_\phi(af + bg) \leq aI_\phi(f) + bI_\phi(g) \leq I_\phi(af + bg) + \varepsilon$$

Then by our prior reasoning there exists $\phi \in C_c^+(G)$ with $\text{supp}(\phi) \subseteq V$ such that $|I(f) - I_\phi(f)| < \varepsilon$, $|I(g) - I_\phi(g)| < \varepsilon$, and $|I(af + bg) - I_\phi(af + bg)| < \varepsilon$. And hence we can get that $|I(af + bg) - aI(f) - bI(g)| < 4\varepsilon$.

By taking $\varepsilon \to 0$ this then proves that $I(af+bg) = aI(f) + bI(g)$.

Similarly, to prove that $I$ is left-invariant let $\varepsilon > 0$ and pick $\phi$ such that $|I(f) - I_\phi(f)| < \varepsilon$ and $|I(L_x f) - I_\phi(L_x f)| < \varepsilon$. Then $|I(f) - I(L_x f)| < 2\varepsilon$.

We can extend $I$ to all of $C_c(G, [0,\infty))$ by defining $I(0) = 0$. This importantly preserves the linearity and left-invariance of $I$. Then similarly to the proof of lemma 7.15 on *pages 57-58*, by setting $I(f) = I(f^+) - I(f^-)$ where $f^+$ and $f^-$ are the positive and negative parts of $f$ we can extend $I$ to being a positive real linear functional on $C_c(G, \mathbb{R})$. And this extension is clearly still left-invariant since $(L_x f)^+ = L_x f^+$ and $(L_x f)^- = L_x f^-$.

Finally, we extend $I$ to being a positive left-invariant linear functional on all of $C_c(G)$ by just setting $I(f) = I(\mathrm{Re}(f)) + iI(\mathrm{Im}(f))$. Then by applying the Riesz-representation theorem plus *proposition 11.4(b)* we get a left Haar measure on $G$. ■

I will go into more depth on Haar measures later on *page ___*.

---

# 10/30/2025

**Math 220a Notes:**

We'll now introduce a notion of symmetric points with respect to a given circle $\Gamma \subseteq \mathbb{C}_\infty$. Firstly, if $\Gamma = \mathbb{R}_\infty := \mathbb{R} \cup \{\infty\}$, then clearly the intuitive definition of a symmetric point of $z \in \mathbb{C}$ would be the point $z^* := \overline{z} \in \mathbb{C}$.

Proposition: If $S$ is a Möbius transformation and $S(\mathbb{R}) = \mathbb{R}$, then $S(z^*) = (S(z))^*$ for all $z \in \mathbb{C}$ with $S(z) \neq \infty$.

Proof:
$S$ is uniquely determined by the points $z_1, z_2, z_3 \in \mathbb{C}_\infty$ such that $S(z_1) = 1$, $S(z_2) = 0$, and $S(z_3) = \infty$. But note that since $S(\mathbb{R}) = \mathbb{R}$ and $S$ maps circles to circles, we know that $z_1, z_2, z_3 \in \mathbb{R}_\infty$. Hence, by our construction in the existence proof at the top of *page 337*, we know that there are real $a, b, c, d \in \mathbb{R}$ such that $S(z) = \frac{az+b}{cz+d}$. And now if $z \in \mathbb{C} - \{z_3\}$, we have that:

$$S(z)^* = \overline{S(z)} = \overline{\left(\frac{az+b}{cz+d}\right)} = \frac{a\overline{z}+b}{c\overline{z}+d} = S(\overline{z}) = S(z^*). \blacksquare$$

Next we consider letting $\Gamma \subseteq \mathbb{C}_\infty$ be any circle. Then we fix $z_1, z_2, z_3 \in \Gamma$ and define the Möbius transformation $T(z) := (z, z_1, z_2, z_3)$. Given any $z \in \mathbb{C}_\infty - \{z_3\}$ we define the symmetric point of $z$ with respect to $\Gamma$ to be $z^* = T^{-1}(\overline{T(z)})$.

In other words, $z^*$ is a symmetric point of $z$ relative to $\Gamma$ iff $(z^*, z_1, z_2, z_3) = \overline{(z, z_1, z_2, z_3)}$.

Claim: Our definition of symmetric point relative to $\Gamma$ is independent of our choice of $z_1, z_2, z_3 \in \Gamma$. In other words, for any $z \in \mathbb{C}_\infty$, if $\{z_1, z_2, z_3\}$ and $\{\widetilde{z_1}, \widetilde{z_2}, \widetilde{z_3}\}$ are two triplets of distinct points in $\Gamma$ with $z_3 \neq z$ and $\widetilde{z_3} \neq z$, then after defining $T_1(z) := (z, z_1, z_2, z_3)$ and $T_2(z) := (z, \widetilde{z_1}, \widetilde{z_2}, \widetilde{z_3})$ we have that $T_1^{-1}(\overline{T_1(z)}) = T_2^{-1}(\overline{T_2(z)})$.

Proof:

Note that $T_1 \circ T_2^{-1} =: M$ sends $\mathbb{R}$ to $\mathbb{R}$, as does $M^{-1} = T_2 \circ T_1^{-1}$. Importantly, we can thus apply our prior proposition to see that $M^{-1}(\overline{w}) = \overline{M^{-1}(w)}$ when $w \in \mathbb{C}$ and $M^{-1}(w) = T_2(T_1^{-1}(w)) \neq \infty$. In particular, if $w = M(T_2(z)) = T_1(z)$ then we have that $M^{-1}(\overline{M(T_2(z))}) = \overline{M^{-1}(M(T_2(z)))}$ if $T_1(z) \neq \infty$ and $T_2(T_1^{-1}(T_1(z))) \neq \infty$.

So for all $z \in \mathbb{C}_\infty - \{z_3, \widetilde{z_3}\}$ we have that:

$$T_1^{-1}(\overline{T_1(z)}) = T_2^{-1}(T_2(T_1^{-1}(\overline{T_1(T_2^{-1}(T_2(z)))})))$$
$$= T_2^{-1}(M^{-1}(\overline{M(T_2(z))})) = T_2^{-1}(\overline{M^{-1}(M(T_2(z)))}) = T_2^{-1}(T_2(z)). \blacksquare$$

As a side note, for any $z \in \mathbb{C}_\infty$ we can always choose $z_3 \in \Gamma$ such that $z \neq z_3$. Hence, we can say that every point $z$ in $\mathbb{C}_\infty$ has a well-defined symmetric point $z^*$ relative to $\Gamma$.

Note that since $z^*$ is the symmetric point of $z$ relative to $\Gamma$ iff $(z^*, z_1, z_2, z_3) = \overline{(z, z_1, z_2, z_3)}$, we clearly have that $(z^*)^* = z$ (relative to $\Gamma$).

(Conway) Theorem III.3.19 (The Symmetry Principle): If a Möbius transformation $T$ takes a circle $\Gamma_1$ onto the circle $\Gamma_2$, then any pair of points symmetric with respect to $\Gamma_1$ are mapped by $T$ onto a pair of points symmetric with respect to $\Gamma_2$.

Proof:
Let $z_2, z_3, z_4$ be distinct points in $\Gamma_1$ such that $z \neq z_4$. Then if $z$ and $z^*$ are symmetric with respect to $\Gamma_1$ we have that:

$$(Tz^*, Tz_2, Tz_3, Tz_4) = (z^*, z_2, z_3, z_4) = \overline{(z, z_2, z_3, z_4)} = \overline{(Tz, Tz_2, Tz_3, Tz_4)}.$$

And since $Tz_2, Tz_3, Tz_4$ are three distinct points of $\Gamma_2$, we have that $Tz^*$ and $Tz$ are symmetric with respect to $\Gamma_2$. $\blacksquare$

Can we get an explicit formula for $z^*$?

Firstly we need a quick observation. If $z_1, z_2, z_3, z_4 \in \mathbb{C}$ with $z_1 \neq z_4$ then:

$$\overline{(z_1, z_2, z_3, z_4)} = (\overline{z_1}, \overline{z_2}, \overline{z_3}, \overline{z_4}).$$

Why?
From the existence proof in the theorem on *page 337* we know that:

$$(z_1, z_2, z_3, z_4) = \tfrac{(z_1 - z_3)(z_2 - z_4)}{(z_1 - z_4)(z_2 - z_3)} \text{ and } (\overline{z_1}, \overline{z_2}, \overline{z_3}, \overline{z_4}) = \tfrac{(\overline{z_1} - \overline{z_3})(\overline{z_2} - \overline{z_4})}{(\overline{z_1} - \overline{z_4})(\overline{z_2} - \overline{z_3})}.$$

Now let $\Gamma = \{z : |z - a| = R\}$ be a circle. Then for any three distinct points $z_2, z_3, z_4$ in $\Gamma$ and $z \in \mathbb{C}$ with $z \neq z_4$ we have (since Mobius transforms preserve cross ratios) that:

$$(z^*, z_2, z_3, z_4) = \overline{(z, z_2, z_3, z_4)}$$
$$= \overline{(z - a, z_2 - a, z_3 - a, z_4 - a)} = \overline{(\tfrac{R^2}{z-a}, \tfrac{R^2}{z_2-a}, \tfrac{R^2}{z_3-a}, \tfrac{R^2}{z_4-a})}$$
$$= (\tfrac{R^2}{\overline{z}-\overline{a}}, \tfrac{R^2}{\overline{z_2}-\overline{a}}, \tfrac{R^2}{\overline{z_3}-\overline{a}}, \tfrac{R^2}{\overline{z_4}-\overline{a}})$$
$$= (\tfrac{R^2}{\overline{z}-\overline{a}}, \tfrac{(z_2-a)(\overline{z_2}-\overline{a})}{\overline{z_2}-\overline{a}}, \tfrac{(z_3-a)(\overline{z_3}-\overline{a})}{\overline{z_3}-\overline{a}}, \tfrac{(z_4-a)(\overline{z_4}-\overline{a})}{\overline{z_4}-\overline{a}})$$
$$= (\tfrac{R^2}{\overline{z}-\overline{a}}, z_2 - a, z_3 - a, z_4 - a)$$
$$= (\tfrac{R^2}{\overline{z}-\overline{a}} + a, z_2, z_3, z_4)$$

Hence $z^* = a + \frac{R^2}{\overline{z}-\overline{a}}$ (when $\Gamma = \{z : |z-a| = R\}$). And in particular we have that $(z^* - a)(\overline{z} - \overline{a}) = R^2$.

Perhaps unsurprisingly this indicates that the symmetric point of the center of the circle is $\infty$.

---

Suppose $\Gamma = \mathbb{R}$ and let $z_1, z_2, z_3 \in \mathbb{R}$. Then put $T(z) = (z, z_1, z_2, z_3) = \frac{az+b}{cz+d}$. As mentioned before we can choose $a, b, c, d$ to be real-valued. Thus:

$$Tz = \frac{az+b}{cz+d} = \frac{az+b}{|cz+d|^2}(c\overline{z} + d) = \frac{1}{|cz+d|^2}(ac|z|^2 + bd + bc\overline{z} + adz)$$

And specifically focusing on the imaginary component, we have that:

$$\mathrm{Im}((z, z_1, z_2, z_3)) = \frac{(ad-bc)}{|cz+d|^2}\mathrm{Im}(z).$$

This shows that $\{z : \mathrm{Im}((z, z_1, z_2, z_3)) < 0\}$ is equal to either $\{z : \mathrm{Im}(z) < 0\}$ or $\{z : \mathrm{Im}(z) > 0\}$ depending on whether $ad - bc > 0$ or $ad - bc < 0$ respectively.

Next suppose $\Gamma$ is an arbitrary circle and that $z_1, z_2, z_3 \in \Gamma$. Then if $S$ is any Möbius transformation we have that:

$$\begin{aligned}\{z : \mathrm{Im}((z, z_1, z_2, z_3)) > 0\} &= \{z : \mathrm{Im}((S(z), S(z_1), S(z_2), S(z_3))) > 0\} \\ &= S^{-1}(\{z : \mathrm{Im}((z, S(z_1), S(z_2), S(z_3))) > 0\})\end{aligned}$$

And in particular, if $S$ maps $\Gamma$ onto $\mathbb{R}_\infty$ then $\{z : \mathrm{Im}((z, z_1, z_2, z_3)) > 0\} = S^{-1}(H)$ where $H \subseteq \mathbb{C}$ is either the upper half plane or lower half plane.

For a circle, we can indicate an orientation (i.e. a direction going around the circle) of the circle by picking an ordered triple $(z_1, z_2, z_3)$ on $\Gamma$. Intuitively, you can think of an orientation as saying that you travel in $\Gamma$ in the direction going from $z_1$ to $z_2$ without passing through $z_3$ in the middle.

If $(z_1, z_2, z_3)$ is an orientation of $\Gamma$ then we define the right side of $\Gamma$ (with respect to our orientation) to be $\{z : \mathrm{Im}((z, z_1, z_2, z_3)) > 0\}$. Similarly, we define the left side of $\Gamma$ to be $\{z : \mathrm{Im}((z, z_1, z_2, z_3)) < 0\}$.

(Conway) Theorem III.3.21 (The Orientation Principle): Let $\Gamma_1$ and $\Gamma_2$ be two circles in $\mathbb{C}_\infty$ and let $T$ be a Möbius transformation such that $T(\Gamma_1) = \Gamma_2$. Let $(z_1, z_2, z_3)$ be an orientation for $\Gamma_1$. Then $T$ takes the right side and the left side of $\Gamma_1$ onto the right side and left side of $\Gamma_2$ with respect to the orientation $(Tz_1, Tz_2, Tz_3)$.

Why? Just note that $(z, z_1, z_2, z_3) = (Tz, Tz_1, Tz_2, Tz_3)$.

---

One more comment I'll make before moving on:

Recall that if $\Gamma \subseteq \mathbb{C}_\infty$ is a circle and $z_1, z_2, z_3 \in \Gamma$, then $f(z) := \mathrm{Im}((z, z_1, z_2, z_3))$ is equal to zero iff $z \in \Gamma$. It follows if $G_+$ denotes the left side of $\Gamma$ relative to $(z_1, z_2, z_3)$ and $G_-$ denotes the right side, $G_+$ and $G_-$ partition $\mathbb{C}_\infty - \Gamma$.

Also note that since $f$ is continuous, we can show that both $G_+$ and $G_-$ are clopen in $\mathbb{C}_\infty - \Gamma$. Since $\mathbb{C}_\infty - \Gamma$ is easily shown to have at most two path components, it follows that both $G_+$ and $G_-$ must be the connected components of $\mathbb{C}_\infty - \Gamma$.

A consequence of this as well as the orientation principle is that if if $T$ maps a circle $\Gamma_1 = \{z : |z-a| = R\}$ to another circle $\Gamma_2 = \{z : |z-a'| = R'\}$, then either $T$ maps the interior $\Gamma_1$ to the whole interior of $\Gamma_2$ or $T$ maps the interior of $\Gamma_1$ to the whole exterior of $\Gamma_2$.

Actually I have another comment to make as well.

By our construction on *page 337*, we know that $(z, z_1, z_2, z_3) = (z, z_1, z_3, z_2)^{-1}$. In particular, since $\frac{1}{w} = \overline{w}|w|^2$, this means that the orientation $(z_1, z_3, z_2)$ has the oppositive left vs right sides as does the orientation $(z_1, z_2, z_3)$.

---

The next topic covered by math 220a is proving Cauchy's formula and then doing a bunch of stuff with that such as proving that holomorphic functions are analytic. Since I already took notes on a bunch of this last Spring, I'm going to intentionally skip over a lot of this.

(Conway) Proposition IV.2.1: Let $\varphi : [a,b] \times [c,d] \to \mathbb{C}$ be a continuous function and define $g : [c,d] \to \mathbb{C}$ by $g(t) = \int_a^b \varphi(s,t)\mathrm{d}s$. Then $g$ is continuous. Moreover, if $\frac{\partial \varphi}{\partial t}(s,t)\mathrm{d}s$ and is continuous on $[a,b] \times [c,d]$ then $g$ is continuously differentiable with $g'(t) = \int_a^b \frac{\partial \varphi}{\partial t}(s,t)\mathrm{d}s$.

Why? Just use the fact that $\varphi$ or $\frac{\partial \varphi}{\partial t}$ is continuous on a compact domain in order to get an upper bound and then apply the theorem from math 240a (see *page 189*).