Now we have characterized when $\mathrm{spt}(\mu^{*n}) = \mathbb{Z}_p$ in terms of μ alone. It turns out that this is also a criterion for ergodicity!

<u>Theorem</u> (Ergodic theorem) A probability distribution μ is ergodic if and only if its support is not contained in a coset of a proper subgroup of $\mathbb{Z}_p$.

Proof: We have already seen that if μ is ergodic there must exist $n \in \mathbb{N}$ with $\mathrm{spt}(\mu^{*n}) = \mathbb{Z}_p$. We must prove the converse: that if $\mathrm{spt}(\mu^{*k}) = \mathbb{Z}_p$ for some k then $\lim_{n\to\infty} \mu^{*n} = \lambda$.

Fix a distribution μ with the property that $\mathrm{spt}(\mu)$ is not contained in a coset of a proper subgroup of $\mathbb{Z}_p$. Define

$$m_k = \min\{\mu^{*k}(t) : t \in \mathbb{Z}_p\} \qquad M_k = \max\{\mu^{*k}(t) : t \in \mathbb{Z}_p\}$$

for all $k \in \mathbb{N}$. Since there is k_0 with $\mathrm{spt}(\mu^{*k_0}) = \mathbb{Z}_p$ we have

$$\varepsilon = m_{k_0} \in (0,1).$$

We will show that both $\lim_{k\to\infty} m_k$ and $\lim_{k\to\infty} M_k$ exist, are equal, and are positive. Convergence follows from monotonicity: we have

$$\mu^{*(k+1)}(t) = \sum_{s\in\mathbb{Z}_p} \mu(t \ominus s)\mu^{*k}(s) \geqslant \sum_{s\in\mathbb{Z}_p} \mu(t\ominus s) m_k = m_k$$

for all $t \in \mathbb{Z}_p$ so $\min\{\mu^{*(k+1)}(t) : t\in\mathbb{Z}_p\} \geqslant m_k$. Similarly

$$\mu^{*(k+1)}(t) = \sum_{s\in\mathbb{Z}_p} \mu(t\ominus s)\mu^{*k}(s) \leqslant \sum_{s\in\mathbb{Z}_p} \mu(t\ominus s) M_k = M_k$$

gives $\max\{\mu^{*(k+1)}(t) : t \in \mathbb{Z}_p\} \leq M_k$. Thus

$$M_{k+1} \leq M_k \qquad\qquad m_k \leq m_{k+1}$$

for all $k \in \mathbb{N}$. Since both sequences are bounded, they converge to M_∞ and m_∞ respectively, say. Both are positive because $m_{k_0} > 0$.

Now lets prove the limits are the same. We calculate that

$$\begin{aligned}
\mu^{*(k_0+r)}(t) &= \sum_{s\in\mathbb{Z}_p} \mu^{*k_0}(t\ominus s)\mu^{*r}(s) \\
&= \sum_{s\in\mathbb{Z}_p} \left(\mu^{*k_0}(t\ominus s) - \varepsilon\mu^{*r}(-s) + \varepsilon\mu^{*r}(-s)\right)\mu^{*r}(s) \\
&= \sum_{s\in\mathbb{Z}_p} \left(\mu^{*k_0}(t\ominus s) - \varepsilon\mu^{*r}(-s)\right)\mu^{*r}(s) + \sum_{s\in\mathbb{Z}_p} \varepsilon\mu^{*r}(-s)\mu^{*r}(s) \\
&= \sum_{s\in\mathbb{Z}_p} \left(\mu^{*k_0}(t\ominus s) - \varepsilon\mu^{*r}(-s)\right)\mu^{*r}(s) + \varepsilon\mu^{*(2r)}(0) \\
&\geq \sum_{s\in\mathbb{Z}_p} \left(\mu^{*k_0}(t\ominus s) - \varepsilon\mu^{*r}(-s)\right)m_r + \varepsilon\mu^{*(2r)}(0) \\
&= (1-\varepsilon)m_r + \varepsilon\mu^{*(2r)}(0)
\end{aligned}$$

because

$$\begin{aligned}
\mu^{*k_0}(t\ominus s) - \varepsilon\mu^{*r}(-s) &\geq \mu^{*k_0}(t\ominus s) - \mu^{*k_0}(t\ominus s)\mu^{*r}(-s) \\
&= \mu^{*k_0}(t\ominus s)\left(1-\mu^{*r}(-s)\right) \geq 0.
\end{aligned}$$

Similarly $\mu^{*(k_0+r)}(t) \leq (1-\varepsilon)M_r + \varepsilon\mu^{*(2r)}(0)$. Since $t\in\mathbb{Z}_p$ was arbitrary we conclude that $m_{k_0+r} \geq (1-\varepsilon)m_r + \varepsilon\mu^{*2r}(0)$ and $M_{k_0+r} \leq (1-\varepsilon)M_r + \varepsilon\mu^{*2r}(0)$. Finally, we have

$$M_{k_0+r} - m_{k_0+r} \leq (1-\varepsilon)(M_r - m_r)$$

and induction gives

$$M_{jk_0+r} - m_{jk_0+r} \leq (1-\varepsilon)^j(M_r - m_r)$$

from which it follows that $M_{jk_0+r} - m_{jk_0+r} \to 0$ as $j\to\infty$.

Lastly, if $m_\infty = M_\infty$ then we must have that $\lim_{n\to\infty}\mu^{*n}$ is constant as a function on $\mathbb{Z}_p$ and, as a distribution, must be λ. $\square$