Theorem. Let $A \subseteq \Sigma^*$. The following statements are equivalent.

1. A is regular. $\exists$ a finite automaton M s.t $L(M) = A$.

2. $A = L(\alpha)$ for some pattern α.

3. $A = L(\alpha)$ for some regular expression α.

$1 \Rightarrow 3$ Given a finite state automaton M, we can construct a regular expression α s.t $L(\alpha) = L(M)$.

Proof:

Let $M = (Q, \Sigma, \Delta, S, F)$ be an NFA without ϵ transitions

For all $Y \subseteq Q$ and $u, v \in Q$ we construct a regular expression α^Y_{uv}

α^Y_{uv} - the set of all strings x such that there is a path from state u to state v in M labelled x [Formally, $v \in \hat{\Delta}(\{u\}, x)$] and all states along the path with possible exception of u and v lie in Y.

Induction on size of Y.

Base Case : $Y = \phi$.

$a_1, a_2, \ldots a_k \in \Sigma$ s.t $v \in \Delta(u, a_i)$

Case 1. $u \neq v$

$$\alpha_{uv}^{\phi} = \begin{cases} a_1 + a_2 + \cdots + a_k & \text{if } k \geq 1. \\ \phi & \text{if } k = 0 \end{cases}$$

Case 2. $u = v$

$$\alpha_{uv}^{\phi} = \begin{cases} a_1 + a_2 + \cdots + a_k + \epsilon & \text{if } k \geq 1 \\ \epsilon & \text{if } k = 0 \end{cases}$$

Induction step.

$$\alpha_{uv}^{Y} = \alpha_{uv}^{Y-\{q\}} + \alpha_{uq}^{Y-\{q\}} \left(\alpha_{qq}^{Y-\{q\}}\right)^{*} \alpha_{qv}^{Y-\{q\}}$$

Choose an arbitrary state $q \in Y$

α - sum of all expressions of the form.

α_{sf}^{Q} where $s \in S$ and $f \in F$.

Let Σ and Γ be finite alphabet sets.

Homomorphism $h: \Sigma^* \to \Gamma^*$ such that $\forall x, y \in \Sigma^*$

$$h(xy) = h(x)h(y) \quad \text{--- (H1)}$$

$$h(\epsilon) = \epsilon \quad \text{--- (H2)}$$

Any homomorphism defined on Σ^* is uniquely determined by its values on Σ.

$\Sigma = \{a, b\}$ $\quad \Gamma = \{c, d, e\}$ $\quad h(a) = cde$, $h(b) = dd$

$h(aab) = cde\,cde\,dd = h(a)\,h(a)\,h(b)$

Any function $h: \Sigma \to \Gamma^*$ extends uniquely (by induction) to a homomorphism defined on Σ^*

For $A \subseteq \Sigma^*$ let $h(A) = \{ h(x) \mid x \in A \} \subseteq \Gamma^*$

For $B \subseteq \Gamma^*$ let $h^{-1}(B) = \{ x \mid h(x) \in B \} \subseteq \Sigma^*$

$h(A)$: image of A under h.

$h^{-1}(B)$: preimage of B under h.

Theorem 2. Let $h : \Sigma^* \to \Gamma^*$ be a homomorphism. if $B \subseteq \Gamma^*$ is regular then $h^{-1}(B)$ is regular.

Proof of Theorem 2. Let $M = (Q, \Gamma, \delta, s, F)$ – DFA

Such that $L(M) = B$. To show: $\exists M'$ over Σ s.t
$L(M') = h^{-1}(B)$.

Definition of M': $M' = (Q, \Sigma, \delta', s, F)$

$$\delta'(\underset{\in \Sigma}{q, a}) = \hat{\delta}(q, \underbrace{h(a)}_{\in \Gamma^*})$$

Lemma 1. $\hat{\delta}'(q, x) = \hat{\delta}(q, h(x))$.

Proof.
Induction on $|x|$. Base case $x = \epsilon$ is trivial.

$$\begin{aligned}
\hat{\delta}'(q, xa) &= \delta'(\hat{\delta}'(q, x), a) && [\text{Def of } \hat{\delta}'] \\
&= \delta'(\hat{\delta}(q, h(x)), a) && [\text{I.H.}] \\
&= \hat{\delta}(\hat{\delta}(q, h(x)), h(a)) && [\text{Def of } \delta'] \\
&= \hat{\delta}(q, h(x) h(a)) \\
&= \hat{\delta}(q, h(xa)) && [\text{property (H1)}]
\end{aligned}$$

Lemma 1. $\hat{\delta}'(q, x) = \hat{\delta}(q, h(x))$

To show $L(M') = h^{-1}(B)$

Suffices to show $L(M') = h^{-1}(L(M))$

For any $x \in \Sigma^*$,

$x \in L(M')$ iff $\hat{\delta}'(s, x) \in F$ [Defn of acceptance]

iff $\hat{\delta}(s, h(x)) \in F$ [Lemma 1]

iff $h(x) \in L(M)$ [Defn. of acceptance]

iff $x \in h^{-1}(L(M))$ [Defn. of $h^{-1}(L(M))$]