Let's review what we've done in the abstract situation. We are studying linear operators $T : V \longrightarrow V$ of a finite-dimensional vector space V. We defined an $\mathbb{F}[z]$-module structure on V in the following way:

Let $p(z) \in \mathbb{F}[z]$ be a polynomial written

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0.$$

Then

$$p(T) = a_n T^n + a_{n-1} T^{n-1} + \cdots + a_1 T + a_0 I$$

is a linear operator on V. We define the action of $\mathbb{F}[z]$ on V by

$$p(z) \cdot v = p(T)v.$$

We denote this $\mathbb{F}[z]$-module by V_T.

Since $\text{End}_{\mathbb{F}}(V)$ is an n^2-dimensional vector space, the set

$$\{I, T, T^2, \ldots, T^{n^2-1}, T^{n^2}\}$$

has $n^2 + 1$ elements and must therefore be linearly dependent. Hence, there exists a set of $a_i \in \mathbb{F}$, not all of which are zero, such that

$$a_{n^2} T^{n^2} + a_{n^2-1} T^{n^2-1} + \cdots + a_1 T + a_0 I = 0$$

which gives us that T vanishes on the polynomial

$$a_{n^2} z^{n^2} + a_{n^2-1} z^{n^2-1} + \cdots + a_1 z + a_0.$$

Define $J := \{p(z) \in \mathbb{F}[z] \mid p(T) = 0\}$. The set J is nonempty, and contains a nonzero polynomial, by our discussion above. One can show that J is an ideal in $\mathbb{F}[z]$, and since $\mathbb{F}[z]$ is a PID, there exists a polynomial of minimal degree that generates J. We call this polynomial the minimal polynomial for T.

1 The $\mathbb{F}[z]$-module structure on X_q

We now wish to use the $\mathbb{F}[z]$-module structure on a vector space to study shift operators. Throughout this discussion, $q(z) \in \mathbb{F}[z]$ is a monic polynomial of positive degree. The map $\pi_q : \mathbb{F}[z] \longrightarrow \mathbb{F}[z]$ is the ring

homomorphism with $\operatorname{Ker}\pi_q = \langle q(z)\rangle$. By the First Isomorphism Theorem,

$$\operatorname{Im}\pi_q \cong \frac{\mathbb{F}[z]}{\langle q(z)\rangle}.$$

We define

$$X_q = \operatorname{Im}\pi_q = \{\pi_q f(z) \mid f(z) \in \mathbb{F}[z]\}$$

and

$$\begin{aligned} S_q : X_q &\longrightarrow X_q \\ f &\longmapsto \pi_q(zf(z)). \end{aligned}$$

This gives us an action $z \cdot f = S_q f(z)$. Notice that for any $\alpha \in \mathbb{F}$ and $f, g \in X_q$ that

$$\begin{aligned} S_q(f + \alpha g) &= \pi_q(z(f + \alpha g)) \\ &= \pi_q(zf + \alpha zg) \\ &= \pi_q(zf) + \pi_q(\alpha zg) \\ &= \pi_q(zf) + \alpha\pi_q(zg) \\ &= S_q(f) + \alpha S_q(g) \end{aligned}$$

and therefore the operator S_q is $\mathbb{F}$-linear. Now,

$$\begin{aligned} z^k \cdot f &= z^{k-1}(z \cdot f) \\ &= z^{k-1} \cdot S_q(f) \\ &= z^{k-1} \cdot S_q^2(F) \end{aligned}$$

and one carries on by induction to conclude that $z^k \cdot f = S_q^k(f)$. Hence, for any $p(z) \in \mathbb{F}[z]$,

$$p(z) \cdot f(z) = p(S_q)f(z) = \pi_q(p(z))$$

which gives us the $\mathbb{F}[z]$-module structure on X_q.

2 A Matrix Representation for S_q

We now proceed to discuss a matrix representation of S_q with respect to the standard basis of X_q. For $0 \leq i \leq n-2$,

$$S_q(z^i) = \pi_q(z^{i+1}) = z^{i+1}$$

because $i+1 < \deg q(z)$. However,

$$S_q(z^{n-1}) = \pi_q(z^n) = -q_{n-1}z^{n-1} - \cdots - q_1(z) - q_0.$$

Since S_q is a linear transformation, it is completely determined by its values on a basis, we get

$$C_q^{\#} := \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & -q_0 \\ 1 & 0 & \cdots & 0 & 0 & -q_1 \\ 0 & 1 & \cdots & 0 & 0 & -q_2 \\ 0 & 0 & \cdots & 0 & 0 & -q_3 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & -q^{n-2} \\ 0 & 0 & \cdots & 0 & 1 & -q^{n-1} \end{pmatrix}.$$

This is the companion matrix for $q(z)$, and one can show that $q(z)$ is the characteristic polynomial for $C_q^{\#}$. These companion matrices will form the building blocks for our classification of linear transformations up to similarity.

Lemma 1. *Let $q(z) \in \mathbb{F}[z]$ be a monic polynomial of degree $n \geq 2$.The characteristic polynomial of the companion matrix $C_q^{\#}$ is $q(z)$.*

Proof. We induct on the degree of the polynomial. If the degree of q is 2, then we can write $q(z) = z^2+q_1z+q_0$. Then

$$\begin{aligned} \det(zI - C_q^{\#}) &= \begin{vmatrix} z & q_0 \\ -1 & z+q_1 \end{vmatrix} \\ &= z(z+q_1) + q_0 \\ &= z^2 + q_1z + q_0 \end{aligned}$$

as desired. Now suppose that the statement holds for $2 \leq k \leq n-1$. Then

$$\det(zI - C_q^{\#}) = \begin{vmatrix} z & 0 & \cdots & 0 & 0 & q_0 \\ -1 & z & \cdots & 0 & 0 & q_1 \\ 0 & -1 & \cdots & 0 & 0 & q_2 \\ 0 & 0 & \cdots & 0 & 0 & q_3 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & z & q_{n-2} \\ 0 & 0 & \cdots & 0 & -1 & z + q_{n-1} \end{vmatrix}$$

$$= z \begin{vmatrix} z & \cdots & 0 & 0 & q_1 \\ -1 & \cdots & 0 & 0 & q_2 \\ 0 & \cdots & 0 & 0 & q_3 \\ \vdots & & \vdots & \vdots & \vdots \\ 0 & \cdots & -1 & z & q_{n-2} \\ 0 & \cdots & 0 & -1 & z + q_{n-1} \end{vmatrix} + \begin{vmatrix} 0 & \cdots & 0 & 0 & q_0 \\ -1 & \cdots & 0 & 0 & q_2 \\ 0 & \cdots & 0 & 0 & q_3 \\ \vdots & & \vdots & \vdots & \vdots \\ 0 & \cdots & -1 & z & q_{n-2} \\ 0 & \cdots & 0 & -1 & z + q_{n-1} \end{vmatrix}$$

$$= z(q_1 + q_2 z + q_3 z^2 + \cdots q_{n-2} z^{n-3} + q_{n-1} z^{n-2} + z^{n-1}) + q_0$$

$$= q(z)$$

as claimed. □

3 Invariant Subspaces

Having a module structure on X_q, a natural question to ask is: What are the submodules? Suppose that $M \subseteq X_q$ is an $\mathbb{F}[z]$-submodule. Then for any $m_1, m_2,$ and $p(z) \in \mathbb{F}[z]$, $m_1 + p(z) \cdot m_2 \in M$. That is,

$$m_1 + p(z) \cdot m_2 = m_1 + p(S_q)m_2 = m_1 + \pi_q(p(z)m_2) \in M$$

which gives us that M is an S_q-invariant subspace. On the other hand, if M is an S_q-invariant subspace, then it is also an $\mathbb{F}[z]$-submodule. The details are not difficult to produce. Our next proposition classifies what the S_q-invariant subspaces look like.

Proposition 1. *A subspace $M \subseteq X_q$ is S_q-invariant if and only if $M = q_1 X_{q_2}$, for a factorization $q(z) = q_1(z)q_2(z)$.*

Proof. "$\Longrightarrow$" Suppose the nontrivial factorization $q(z) = q_1(z)q_2(z)$ and consider $M = q_1 X_{q_2}$. Let $f(z) \in M$, and write $f(z) = q_1(z)f_1(z)$, where $\deg f_1 < \deg q_2$. With respect to $q_2(z)$ we have

$$zf_1(z) = a(z)q_1(z) + r(z).$$

Furthermore,

$$\begin{aligned} zf(z) &= zf_1(z)q_1(z) \\ &= (a(z)q_2(z) + r(z))q_1(z) \\ &= a(z)q_1(z)q_2(z) + q_1(z)r(z) \end{aligned}$$

and we have that

$$\begin{aligned} S_q f(z) &= \pi_q(zf(z)) \\ &= q_1(z)r(z) \\ &= q_1(z)\pi_{q_2}(zf_1(z)) \\ &= q_1(z)S_{q_2}(f_1(z)) \in M. \end{aligned}$$

We conclude that M is S_q-invariant.

Now suppose that $\overline{M}$ is an S_q-invaraint subspace of X_q. Then there exists $M \subseteq \mathbb{F}[z]$ such that $M = \pi_q^{-1}(\overline{M})$. It is clear that M is closed under addition. Let $f \in M$. Then we can write $f(z) = f_1(z) + a(z)q(z)$.

So, $zf(z) = zf_1(z) + a'(z)q(z)$ and $\pi_q(zf) = S_q(f_1) \in \overline{M}$. We conclude that M is an ideal of $\mathbb{F}[z]$. Let q_1 be the generator for M. It follows that we can write $q(z) = q_1(z)q_2(z)$ and

$$\overline{M} = \pi_q(M) = \pi_q(\langle q_1(z) \rangle) = q_1 X_{q_2}.$$

□

Now that we know what the invariant subspaces are, we would like to understand how S_q behaves when restricted to an invariant subspace.

Proposition 2. *Let $q(z) = q_1(z)q_2(z)$ be a nontrivial factorization. Then S_q restricted to $q_1 X_{q_2}$ is similar to the shift operator S_{q_2}.*

Proof. Let

$$\begin{aligned} \Phi : X_{q_2} &\longrightarrow q_1 X_{q_2} \\ f &\longmapsto q_1 f \end{aligned}$$

and observe that this is an isomorphism of the two spaces. For $f(z) \in X_{q_2}$,

$$\begin{aligned} (\Phi \circ S_{q_2}) &= q_1 S_{q_2} f \\ &= q_1 \pi_{q_2}(zf) \\ &= \pi_q(z q_1 f) \\ &= S_q(\Phi \circ f). \end{aligned}$$

We conclude that the following diagram commutes:

$$\begin{array}{ccc} X_{q_2} & \xrightarrow{\Phi} & q_1 X_{q_2} \\ \Big\downarrow{\scriptstyle S_{q_2}} & & \Big\downarrow{\scriptstyle S_q|_{q_1 X_{q_2}}} \\ X_{q_2} & \xrightarrow[\Phi]{} & q_1 X_{q_2} \end{array}$$

and since Φ is an isomorphism the statement follows. □

3.1 A Digression: Rewriting π_q

Recall that we have the direct sum decomposition

$$\mathbb{F}((z^{-1})) = \mathbb{F}[z] \oplus z^{-1}\mathbb{F}[[z^{-1}]]$$

and π_+, π_- are the respective canonical projections.

If $f(z) \in \mathbb{F}[z]$ is a nonzero polynomial, then we can write uniquely

$$f(z) = a(z)q(z) + r(z)$$

where $\deg r < \deg q$. Well,

$$q(z)^{-1}f(z) = a(z) + q(z)^{-1}r(z)$$

and applying π_-, we have that

$$\pi_- q^{-1} f = \pi_- q^{-1} r = q^{-1} r.$$

We conclude that

$$\pi_q f = q\pi_- q^{-1} f.$$

We will use this to prove our next theorem.

Theorem 1. *Let $p(z)$ and $q(z)$ be polynomials with $q(z)$ monic and of positive degree. Define*

$$r(z) = \gcd(p, q)$$
$$s(z) = \operatorname{lcm}(p, q).$$

We have the factorizations

$$q(z) = r(z)q_1(z)$$
$$p(z) = r(z)p_1(z)$$

with $\gcd(p_1, q_1) = 1$[1]. *Further,*

$$s(z) = r(z)p_1(z)q_1(z) = p(z)q_1(z) = q(z)p_1(z).$$

Moreover,

$$\operatorname{Ker} p(S_q) = q_1 X_r$$
$$\operatorname{Im} p(S_q) = r X_{q_1}$$

Proof. That p and q can be factored this way and that $\gcd(p_1, q_1) = 1$ is a consequence of the fact that $r(z) = \gcd(p, q)$ and that $\mathbb{F}[z]$ is a PID.

We know that $q_1 X_r$ and $r X_{q_1}$ are S_q-invariant subspaces of X_q from our previous discussion.

Suppose that $f(z) \in q_1 X_r$. Then we can write $f(z) = q_1(z)g(z)$ with $g \in X_r$. We compute

$$\begin{aligned} p(S_q)f &= \pi_q(pf) \\ &= q\pi_- q^{-1} pf \\ &= r q_1 \pi_- r^{-1} q^{-1} r p_1 q_1 g \\ &= r q_1 \pi_- p_1 g \\ &= 0 \end{aligned}$$

and we conclude that $q_1 X_r \subseteq \operatorname{Ker} p(S_q)$.

Conversely, suppose that $f(z) \in \operatorname{Ker} p(S_q)$. Then $\pi_q(pf) = 0$, and there exists $g(z)$ such that $p(z)f(z) = q(z)g(z)$. This implies that

$$r(z)p_1(z)f(z) = r(z)q_1(z)g(z).$$

By left cancellation, $\mathbb{F}[z]$ is a domain,

$$p_1(z)f(z) = q_1(z)g(z)$$

and since $\gcd(p_1, q_1) = 1$, we can conclude that $q_1 \mid f$. That is, we can write

$$f(z) = q_1(z)f_1(z) \quad \text{for some } f_1.$$

[1]This is notation abuse. To say that two polynomials are coprime, one means that the greatest common divisor is any nonzero constant polynomial

Since $f \in X_q$ and $q(z) = r(z)q_1(z)$, we have that $\deg f_1 < \deg r$ and therefore $f_1 \in X_r$. Hence, $\operatorname{Ker} p(S_q) \subseteq q_1 X_r$. This gives us the equality $\operatorname{Ker} p(S_q) = q_1 X_r$.

Now assume that $g(z) \in \operatorname{Im} p(S_q)$. Then there exists $f(z) \in X_q$ such that $p(S_q)f(z) = g(z)$. In other words, $\pi_q(p(z)f(z)) = g(z)$. Then

$$\begin{aligned} g(z) &= \pi_q(p(z)f(z)) \\ &= q\pi_- q^{-1} pf \\ &= q_1 r \pi_- r^{-1} q^{-1} r p_1 f \\ &= q_1 r \pi_- q_1^{-1} p_1 f \\ &= r \pi_{q_1} p_1 f \end{aligned}$$

which is certainly an element of rX_{q_1}.

Now suppose that $g \in rX_{q_1}$. Write $g(z) = r(z)g_1(z)$, for some $g_1 \in X_{q_1}$. By the fact that $\gcd(p_1, q_1) = 1$, the map $f_1 \mapsto \pi_{q_1} p_1 f_1$ acting in X_{q_1} is an invertible map. Hence, there exists $f_1 \in X_{q_1}$ such that $g_1 = \pi_{q_1}(p_1 f_1)$. Now,

$$r g_1 = r q_1 \pi_- r^{-1} q_1^{-1} p_1 r f_1 = \pi_q p r f_1$$

which implies the desired inclusion. □

Theorem 2. *With the same setup of the previous theorem, the linear transformation $p(S_q)$ is invertible if and only if $p(z)$ and $q(z)$ are coprime. Moreover, we have*

$$p(S_q)^{-1} = a(S_q),$$

where the polynomial $a(z)$ arises out of any solution to the Bezout equation

$$a(z)p(z) + b(z)q(z) = 1.$$

Proof. Since $p(z)$ and $q(z)$ are coprime, there exist polynomials $a(z), b(z)$ such that

$$a(z)p(z) + b(z)q(z) = 1.$$

Then

$$a(S_q)p(S_q) + b(S_q)q(S_q) = I$$

which reduces to $a(S_q)p(S_q) = I$ because the characteristic polynomial of S_q is $q(z)$.

We now embark on proving the biconditional.

Injectivity: Notice that

$$0 = \operatorname{Ker} p(S_q) = q_1 X_r$$

if and only if X_r is the trivial subspace. This readily implies that $\gcd(p, q) = r$ is a constant polynomial.

Surjectivity: If $\gcd(p, q) = r$ is a constant polynomial, then $X_q = X_{q_1}$ from the factorization $q(z) = r(z)q_1(z)$. On the other hand, if $X_q = rX_{q_1}$, then we can write $z^{n-1} = r(z)f_1(z)$ where $f_1 \in X_{q_1}$. Then

$$n - 1 = \deg r + \deg f_1 < \deg r + \deg q_1 = n - 1$$

and we conclude that $\deg f_1 = \deg q_1$ and $\deg r = 0$. The statement follows. □

We end this section with a small fact regarding invariant subspaces.

Lemma 2. *Let $q(z)$ be a monic polynomial of positive degree. If $q(z) = q_1(z)q_2(z) = p_1(z)p_2(z)$ are two factorizations, then $q_1X_{q_2} \subseteq p_1X_{p_2}$ if and only if $p_1 \mid q_1$ or $q_2 \mid p_2$.*

Proof. Suppose $p_1 \mid q_1$. Then we can write $q_1(z) = p_1(z)s(z)$, for some polynomial $s(z)$. We have

$$q(z) = q_1(z)q_2(z) = p_1(z)s(z)q_2(z) = p_1(z)p_2(z)$$

and in particular $p_2(z) = s(z)q_2(z)$. This yields

$$q_1X_{q_2} = p_1sX_{q_2} \subseteq p_1X_{sq_2} = p_1X_{p_2}.$$

□

4 Direct Sum Decompositions

Lemma 3. *Let $q(z) = q_1(z)q_2(z)$ be a nontrivial factorization. We have the direct sum decomposition*

$$X_q = X_{q_1} \oplus q_1 X_{q_2}.$$

Proof. Note that $\deg q_1 < \deg q$. This gives us that $X_{q_1} \subseteq X_q$. Every element of X_{q_1} has degree strictly less than q_1 by construction. In a similar vein, every element of $q_1 X_{q_2}$ has degree strictly larger than q_1. This gives us that $X_{q_1} \cap q_1 X_{q_2} = \{0\}$. Now,

$$\begin{aligned} \dim X_q &= \deg q \\ &= \deg q_1 + \deg q_2 \\ &= \dim X_{q_1} + \dim X_{q_2} \end{aligned}$$

which is the dimension of the direct sum. □

Proposition 3. *1. Suppose that $s(z) = \operatorname{lcm}(p_i)$ and $r(z) = \gcd(q_i)$. Then*

$$sX_r = \bigcap_{i=1}^{s} p_i X_{q_i}.$$

2. Suppose that $u(z) = \operatorname{lcm}(q_i)$ and $v(z) = \gcd(p_i)$. Then

$$vX_u = \sum_{i=1}^{s} p_i X_{q_i}.$$

Corollary 1. *Given a nontrivial factorization $q(z) = \prod_{i=1}^{s} p_i(z)q_i(z)$,*

1. The $p_i(z)$ are coprime if and only if

$$X_q = p_1 X_{q_1} + p_2 X_{q_2} + \cdots + p_x X_{q_s}.$$

2. The sum in (1) is a direct sum if and only if the q_i are mutually coprime.

3. We have the direct sum decomposition

$$X_q = p_1 X_{q_1} \oplus p_2 X_{q_2} \oplus \cdots \oplus p_s X_{q_s}$$

if and only if the q_i are mutually coprime and $q(z) = \prod_{i=1}^{s} q_i(z)$ and $p_i(z) = \prod_{j \neq i} q_j(z)$.

Proof. From the classification of S_q-invariant subspaces, we can represent the sum

$$p_1 X_{q_1} + p_2 X_{q_2} + \cdots + p_s X_{q_s} = r X_s$$

Applying the previous proposition, statement 2, $r(z) = \gcd(p_i)$ and $s(z) = \operatorname{lcm}(q_i)$. Hence, $rX_s = X_q$ if and only if $r(z)$ is a constant polynomial, or equivalently $s(z) = q(z)$.

For the second statement, the sum is a direct sum if and only if, for each index i,

$$p_i X_{q_i} \bigcap \left(\sum_{j \neq i} p_j X_{q_j} \right) = 0.$$

Since $\sum_{j \neq i} p_j X_{q_j}$ is an invariant subspace, it can be represented as rX_s, for two polynomials $r(z), s(z)$ such that $q(z) = r(z)s(z)$. Now, with $r(z) = \gcd_{j \neq i}(p_j)$ and $\operatorname{lcm}_{j \neq i}(q_j)$ if and only if $\gcd(s, q_i) = 1$. That is, the q_i are mutually coprime.

The third statement follows from the fact that the p_i are all coprime by construction and the previous statements. □

Corollary 2. *Let $p(z) = p_1(z)^{e_1} p_2(z)^{e_2} \cdots p_k(z)^{e_k}$ be the factorization into irreducibles of the polynomial $p(z)$. Define $s_i(z) = \prod_{j \neq i} p_j(z)^{e_j}, 1 \leq i \leq k$. Then*

$$X_p = s_1 X_{p_1^{e_1}} \oplus s_2 X_{p_2^{e_2}} \oplus \cdots \oplus s_k X_{p_k^{e_k}}.$$

Proof. The $\gcd(s_i) = 1$ and $\operatorname{lcm}(p_i^{e_i}) = p(z)$ by construction. Apply the previous corollary to get the statement. □

5 Eigenvalues and Eigenvectors

Proposition 4. *Let $q(z)$ be a monic polynomial of positive degree. Then*

1. *The eigenvalues of S_q coincide with the zeros of $q(z)$.*
2. *The vector $f(z) \in X_q$ is an eigenvector for S_q corresponding to an eigenvalue λ if and only if it can be written*
$$f(z) = \frac{cq(z)}{z - \lambda}.$$

Proof. Let $f(z)$ be an eigenvector of S_q corresponding to an eigenvalue λ. That is $S_q f(z) = \lambda f(z)$. There exists some scalar $c \in \mathbb{F}$ such that

$$zf - cq = S_q f(z).$$

Then

$$zf(z) - cq(z) = \lambda f(z)$$

and we see that $q(\lambda) = 0$.

Conversely, suppose that λ is a zero of $q(z)$. Then $(z - \lambda) \mid q(z)$ one sees that

$$f(z) = \frac{cq(z)}{z - \lambda} \in X_q.$$

The computation

$$\begin{aligned}(S_q - \lambda I)f(z) &= zf - cq(z) - \lambda f(z) \\ &= (z - \lambda)f(z) - cq(z)\end{aligned}$$

can be applied to obtain the following

$$\begin{aligned}(S_q - \lambda I)f(z) &= \pi_q(z - \lambda)\frac{cq(z)}{z - \lambda} \\ &= \pi_q cq(z) \\ &= 0\end{aligned}$$

We conclude that $f(z) = \frac{cq(z)}{z-\lambda}$ is an eigenvector associated to λ. □

6 Cyclic Transformations and Diagonalization

Definition 1. Let V be an n-dimensional vector space over the field $\mathbb{F}$, and $T : V \longrightarrow V$ a linear operator. We say that T is *cyclic* if there exists $v \in V$ such that the set

$$\{v, Tv, T^2v, \ldots, T^{n-1}v\}$$

is a basis for V. The vector v is said to be a *cyclic vector* for T.

Lemma 4. *Let $q(z) \in \mathbb{F}[z]$ be a monic polynomial of positive degree, and $f(z) \in X_q$. Then*

1. *Them smallest S_q-invariant subspace of X_q containing $f(z)$ is $q_1 X_{q_2}$, where $q(z) = q_1(z)q_2(z)$.*
2. *S_q is a cyclic transformation in X_q.*
3. *A polynomial $f(z) \in X_q$ is a cyclic vector for S_q if and only if $f(z)$ and $q(z)$ are coprime.*

Proof. Let $M \leq X_q$ be the subspace spanned by $\{S_q^i f \mid i \geq 0\}$. This space is clearly S_q-invariant and contains $f(z)$. We've seen that such a space must have the form $q_1 X_{q_2}$, for a nontrivial factorization $q(z) = q_1(z)q_2(z)$. We conclude that there exists $f_1 \in X_{q_2}$ such that $f(z) = q_1(z)f_1(z)$. Hence, q_1 is a divisor of both f and q.

Claim: $q_1 = \gcd(f, q)$.

Suppose that $q_0(z)$ is some common divisor of $f(z)$ and $q(z)$. We can then write $q(z) = q_0(z)q'(z)$ and $f(z) = q_0(z)f'(z)$. Well,

$$S_q^k f = \pi_q z^k f = \pi_q z^k q_0 f' = q_0 \pi_{q'} z^k f = q_0(z) S_{q'}^k f(z)$$

and therefore $q_1 X_{q_2} \subseteq q_0 X_{q'}$ which implies that $q_0 \mid q_1$. One concludes that any common divisor divides $q_1(z)$, from which the claim follows.

For the second statement, we know that $1 \in X_q$. Notice that

$$S_q^k 1 = \pi_q z^k \cdot 1 = z^k \quad \text{for } 0 \leq k < \deg q(z).$$

Hence, the set

$$\{1, S_q 1, S_q^2 1, \ldots, S_q^{n-1} 1\} = \{1, z, z^2, \ldots, z^{n-1}\}$$

is a basis for X_q. We conclude that S_q is a cyclic operator.

To prove the third statement, we note that

$$\dim q_1 X_{q_2} = \dim X_{q_2} = \deg q_2.$$

Now $X_q = q_1 X_{q_2}$ if and only if $\deg q_1(z) = 0$. That is, f and g are relatively prime. We've implicitly used the setup of the proof of (1) here. □

Proposition 5. *Let $q(z)$ be a monic polynomial of positive degree n. Then S_q is diagonalizable if and only if $q(z)$ splits into the product of n distinct linear factors.*

Proof. "$\Longrightarrow$" Suppose that $q(z)$ splits into n distinct linear factors, $q(z) = \prod_{i=1}^{n}(z - \alpha_i)$. Define

$$p_i(z) := \frac{q(z)}{z - \alpha_i} = \prod_{j \neq i}(z - \alpha_j)$$

and recall that the p_i, $q \leq i \leq n$, is the spectral basis for X_q. Now, we've witnessed that α_i is an eigenvalue of S_q and the eigenvector associated to α_i is $\frac{cq(z)}{z-\alpha_i} = cp_i(z)$. The computation

$$\begin{aligned}(S_q - \alpha_i I)(cp_i) &= S_q(cp_i) - \alpha_i cp_i \\ &= cS_q(p_i) - c\alpha_i p_i \\ &= 0,\end{aligned}$$

which gives us that $S_q(p_i) = \alpha_i p_i$. We've now enough to conclude that

$$[S_q]_{\text{sp}}^{\text{sp}} = \begin{pmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_n \end{pmatrix}$$

which is diagonal.

Conversely, suppose that S_q is diagonalizable. Then there exists a basis for which

$$S_q = \text{diag}(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Because S_q is cyclic its minimal polynomial and characteristic polynomial coincide. It is then necessary that all of the α_i are distinct. □