

## SEMISIMPLICITY

KEITH CONRAD

A subspace  $W$  of an  $F$ -vector space  $V$  always has a complementary subspace:  $V = W \oplus W'$  for some subspace  $W'$ . This can be seen using bases: extend a basis of  $W$  to a basis of  $V$  and let  $W'$  be the span of the part of the basis of  $V$  not originally in  $W$ . Of course there are many ways to build a complementary subspace, since extending a basis is a rather flexible procedure. If the vector space or subspace has extra structure then we can ask if a complement to  $W$  can be found with properties related to this structure. For example, when  $V = \mathbf{R}^n$  we have the concept of orthogonality in  $\mathbf{R}^n$ , and any subspace  $W$  has an orthogonal complement:  $\mathbf{R}^n = W \oplus W'$  where  $W \perp W'$ , and moreover there is only one such complement to  $W$ . The orthogonal complement is tied up with the geometry of  $\mathbf{R}^n$ . Another kind of structure we can put on subspaces (of general vector spaces) is stability under a linear operator on the whole space. Given a linear operator  $A: V \rightarrow V$ , a subspace  $W$  satisfying  $A(W) \subset W$  is called an *A-stable* subspace. For example, a one-dimensional *A-stable* subspace is the same thing as the line spanned by an eigenvector for  $A$ : if  $W = Fv$  is *A-stable* then  $A(v) = \lambda v$  for some  $\lambda \in F$ , so  $v$  is an eigenvector. We ask: does an *A-stable* subspace have a complement which is also *A-stable*?

**Example 1.** If  $A = \text{id}_V$  then all subspaces are *A-stable*, so any complement to an *A-stable* subspace is also *A-stable*. In particular, an *A-stable* complement to a subspace is not unique (if the subspace isn't  $\{0\}$  or  $V$ ).

**Example 2.** Consider  $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  acting on  $F^2$  and its eigenspace  $W = \left\{ \begin{pmatrix} x \\ 0 \end{pmatrix} : x \in F \right\}$ . This is *A-stable*. A complementary subspace to  $W$  would be 1-dimensional and thus also be spanned by an eigenvector for  $A$ , but  $W$  is the only eigenspace of  $A$ . So  $W$  is *A-stable* but has no *A-stable* complement. Remember this example!

*From now on, all linear operators are acting on nonzero finite-dimensional vector spaces.*

While a subspace stable for an operator does not always have a stable complementary subspace, we will show any stable subspace has a stable complementary subspace when the operator is potentially diagonalizable. We will carry out the proof in the diagonalizable case first since the ideas are a simpler there, and then one appreciates more clearly the extra details that crop up in the more general potentially diagonalizable case.

**Theorem 3.** *Let  $A: V \rightarrow V$  be diagonalizable and  $V = \bigoplus_{i=1}^r E_{\lambda_i}$  be the corresponding eigenspace decomposition.*

- (1) *If  $W$  is an  $A$ -stable subspace of  $V$  then  $W = \bigoplus_{i=1}^r (W \cap E_{\lambda_i})$  and each  $W \cap E_{\lambda_i}$  is  $A$ -stable,*
- (2) *Any  $A$ -stable subspace of  $V$  has an  $A$ -stable complement.*

*Proof.* (1) We will show  $W = \sum_{i=1}^r (W \cap E_{\lambda_i})$ ; the sum is automatically direct since the subspaces  $E_{\lambda_i}$ 's are linearly independent. (Eigenvectors for different eigenvalues are linearly independent.)

For  $w \in W$ , write  $w = w_1 + \cdots + w_r$  with  $w_i \in E_{\lambda_i}$ . We will show the eigencomponents  $w_i$  all lie in  $W$ , so  $w_i \in W \cap E_{\lambda_i}$  for all  $i$  and thus  $W = \sum_{i=1}^r (W \cap E_{\lambda_i})$ . The reason  $w_i \in W$  is

that  $W$  is  $h(A)$ -stable for any  $h(T) \in F[T]$  since  $W$  is  $A$ -stable, and in the proof that  $V$  has an eigenspace decomposition for  $A$  it is shown that  $w_i = h_i(A)(w)$  for a certain polynomials  $h_i(T) \in F[T]$ . Since  $W$  and  $E_{\lambda_i}$  are both  $A$ -stable, so is their intersection  $W \cap E_{\lambda_i}$ .

(2) Let  $W$  be  $A$ -stable and  $W_i = W \cap E_{\lambda_i}$ , so  $W = \bigoplus_{i=1}^r W_i$  by (1). In each  $E_{\lambda_i}$ ,  $A$  acts by scaling by  $\lambda_i$ , so *all* subspaces of  $E_{\lambda_i}$  are  $A$ -stable. (Not all subspaces of the whole space  $V$  are  $A$ -stable!) Let  $W'_i$  be *any* subspace complement to  $W_i$  inside  $E_{\lambda_i}$ . Then  $W' := \sum_{i=1}^r W'_i = \bigoplus_{i=1}^r W'_i$  is a subspace of  $V$  that is  $A$ -stable (because each  $W'_i$  is  $A$ -stable) and

$$W \oplus W' = \bigoplus_{i=1}^r (W_i \oplus W'_i) = \bigoplus_{i=1}^r E_{\lambda_i} = V.$$

□

Although a potentially diagonalizable operator  $A: V \rightarrow V$  may not have eigenspaces in  $V$ , its minimal polynomial has distinct irreducible factors and we can use them to extend the previous theorem to the potentially diagonalizable case.

**Theorem 4.** *Let  $A: V \rightarrow V$  be potentially diagonalizable, with minimal polynomial  $m_A(T)$ . For each monic irreducible factor  $\pi_i(T)$  of  $m_A(T)$ , let  $V_i = \{v \in V : \pi_i(A)(v) = 0\}$ .*

- (1) *Each  $V_i$  is  $A$ -stable and  $V = \bigoplus_{i=1}^r V_i$ .*
- (2) *If  $W$  is an  $A$ -stable subspace of  $V$  then  $W = \bigoplus_{i=1}^r (W \cap V_i)$  and each  $W \cap V_i$  is  $A$ -stable.*
- (3) *Any  $A$ -stable subspace of  $V$  has an  $A$ -stable complement.*

If  $A$  is diagonalizable, so each  $\pi_i(T)$  is linear, say  $\pi_i(T) = T - \lambda_i$ , then  $V_i = E_{\lambda_i}$  is an eigenspace and this theorem becomes Theorem 3.

*Proof.* (1) Since  $A$  and  $\pi_i(A)$  commute, if  $v \in V_i$  then  $A(v) \in V_i$ . Therefore  $A(V_i) \subset V_i$  for all  $i$ , so each  $V_i$  is  $A$ -stable.

We will show that it is possible to “project” from  $V$  to  $V_i$  using a polynomial in the operator  $A$ . We seek  $h_1(T), \dots, h_r(T)$  in  $F[T]$  such that

$$(1) \quad 1 = h_1(T) + \dots + h_r(T), \quad h_i(T) \equiv 0 \pmod{m_A(T)/\pi_i(T)}.$$

Once these polynomials are found,  $\pi_i(T)h_i(T)$  is divisible by  $m_A(T)$  for all  $i$ , so  $\pi_i(A)h_i(A) = 0$ . Then replacing  $T$  with the operator  $A$  in (1) and applying all operators to any  $v \in V$  gives

$$v = h_1(A)(v) + \dots + h_r(A)(v), \quad \pi_i(A)h_i(A)(v) = 0.$$

The second equation tells us  $h_i(A)(v) \in V_i$ , so the first equation shows  $V = V_1 + \dots + V_r$ . To show this sum is direct, suppose

$$(2) \quad v_1 + \dots + v_r = 0$$

with  $v_i \in V_i$ . We want to show each  $v_i$  is 0. Apply  $h_i(A)$  to both sides of (2). Since  $h_i(T)$  is divisible by  $\pi_j(T)$  for  $j \neq i$ ,  $h_i(A)(v_j) = 0$  for  $j \neq i$  (look at the definition of  $V_j$ ). Therefore  $h_i(A)(v_i) = 0$ . Also  $\pi_i(A)(v_i) = 0$  by the definition of  $V_i$ , so  $h_j(A)(v_i) = 0$  for  $j \neq i$ . Thus  $\text{id}_V = h_i(A) + \sum_{j \neq i} h_j(A)$  kills  $v_i$ , so  $v_i = 0$ .

It remains to find polynomials  $h_i(T)$  fitting (1). Set  $f_i(T) = m_A(T)/\pi_i(T)$ . These polynomials are relatively prime as an  $r$ -tuple, so some  $F[T]$ -linear combination of them is 1:

$$1 = g_1(T)f_1(T) + \dots + g_r(T)f_r(T).$$

Use  $h_i(T) = g_i(T)f_i(T)$ .

(2) We will show  $W = \sum_{i=1}^r (W \cap V_i)$ . Then the sum must be direct because the  $V_i$ 's are linearly independent by (1). For  $w \in W$ , the proof of (1) shows that the component of  $w$  in  $V_i$  is  $w_i := h_i(A)(w)$  for some polynomial  $h_i(T)$ . Since  $W$  is  $A$ -stable and  $h_i(A)$  is a polynomial in  $A$ ,  $w_i \in W$ . Therefore  $w_i \in W \cap V_i$ . Since  $W$  and  $V_i$  are each carried into themselves by  $A$ , so is  $W \cap V_i$ .

(3) This will be more technical than the proof of the corresponding case for diagonalizable operators.

Let  $W$  be  $A$ -stable and set  $W_i := W \cap V_i$ , so  $W = \bigoplus_{i=1}^r W_i$  and the  $W_i$ 's are  $A$ -stable by (2). To find an  $A$ -stable complement to  $W$  in  $V$  it suffices (in fact, it is equivalent) to find an  $A$ -stable complement to  $W_i$  in  $V_i$  for all  $i$ . Then the sum of these complements will be an  $A$ -stable complement to  $W$  in  $V$ . Unlike in the proof of Theorem 3(2),  $A$  need not be a scaling operator on  $V_i$ , so a random subspace complement to  $W_i$  in  $V_i$  is unlikely to be  $A$ -stable. We have to think more carefully to find an  $A$ -stable complement of  $W_i$  in  $V_i$ .

Think about  $V_i$  as an  $F[T]$ -module where any  $f(T) \in F[T]$  acts on  $V$  by  $f(T)(v) := f(A)(v)$ . Since  $A(W_i) \subset W_i$ ,  $W_i$  is an  $F[T]$ -submodule of  $V_i$ . More generally, the  $F[T]$ -submodules of  $V_i$  are precisely the  $A$ -stable  $F$ -vector spaces in  $V$ . We seek an  $F[T]$ -submodule  $W'_i$  of  $V_i$  such that  $V_i = W_i \oplus W'_i$ . Since  $\pi_i(T)$  kills  $V_i$ ,  $V_i$  is an  $F[T]/(\pi_i)$ -module and  $W_i$  is an  $F[T]/(\pi_i)$ -submodule. Now  $F[T]/(\pi_i)$  is a *field*, so  $V_i$  is a vector space over  $F[T]/(\pi_i)$  and  $W_i$  is a subspace over this field. Set  $W'_i$  to be any complementary subspace to  $W_i$  inside  $V_i$  as  $F[T]/(\pi_i)$ -vector spaces. (When  $\det \pi_i > 1$ , this is a stronger condition than being a complementary subspace in  $V_i$  as  $F$ -vector spaces.) Since  $W'_i$  is an  $F[T]/(\pi_i)$ -submodule of  $V_i$ , it is an  $F$ -vector space and  $A$ -stable, so we are done:  $W' = \sum_{i=1}^r W'_i$  is an  $A$ -stable complement to  $W$  in  $V$ .  $\square$

**Definition 5.** A linear operator  $A: V \rightarrow V$  is called *semisimple* if every  $A$ -stable subspace of  $V$  admits an  $A$ -stable complement: when  $W \subset V$  and  $A(W) \subset W$ , we can write  $V = W \oplus W'$  for some subspace  $W'$  such that  $A(W') \subset W'$ .

The term “semisimple” is derived from the term “simple,” so let’s explain what simple means and how semisimple operators are related to simple operators.

**Definition 6.** A linear operator  $A: V \rightarrow V$  is called *simple* when  $V \neq \{0\}$  and the only  $A$ -stable subspaces of  $V$  are  $\{0\}$  and  $V$ .

**Example 7.** A 90-degree rotation of  $\mathbf{R}^2$  is simple because no 1-dimensional subspace of  $\mathbf{R}^2$  is brought back to itself under such a rotation. More generally, any rotation of  $\mathbf{R}^2$  is simple except by 0 degrees and 180 degrees.

**Example 8.** A scalar operator is simple only on a 1-dimensional space.

**Example 9.** On a complex vector space of dimension greater than 1, no linear operator is simple since an eigenvector for the operator spans a 1-dimensional stable subspace.

If  $A: V \rightarrow V$  is semisimple, it turns out that  $V = W_1 \oplus \cdots \oplus W_k$  where each  $W_i$  is  $A$ -stable and  $A$  is simple as an operator on each  $W_i$  (that is, there are no  $A$ -stable subspaces of  $W_i$  besides  $\{0\}$  and  $W_i$ ). So a semisimple operator on  $V$  is a direct sum of simple operators (acting on the different parts of a suitable direct sum decomposition of  $V$ ). We’ll see why there is such a direct sum decomposition in Corollary 12.

The next theorem characterizes semisimplicity of an operator in terms of the minimal polynomial.

**Theorem 10.** *The operator  $A: V \rightarrow V$  is semisimple if and only if its minimal polynomial in  $F[T]$  is squarefree.*

*Proof.* In the proof of Theorem 4, the property we used of  $m_A(T)$  is that it is a product of distinct monic irreducibles, *i.e.*, that it is squarefree in  $F[T]$ . We did not really use that  $m_A(T)$  is separable, which is a stronger condition than being squarefree. (For example, in  $\mathbf{F}_p(u)[T]$ ,  $T^p - u$  is irreducible, so squarefree, but is not separable.) Therefore in the proof of Theorem 4 we already showed an operator with squarefree minimal polynomial is semisimple and all the conclusions of Theorem 4 apply to such an operator.

Now assume  $A$  has a minimal polynomial which is *not* squarefree. We will construct a subspace of  $V$  which is  $A$ -stable but has *no*  $A$ -stable complement. Let  $\pi(T)$  be an irreducible factor of  $m_A(T)$  with multiplicity greater than 1, say  $m_A(T) = \pi(T)^e g(T)$  where  $e \geq 2$  and  $g(T)$  is not divisible by  $\pi(T)$ . Since  $m_A(A) = O$ , every vector in  $V$  is killed by  $\pi(A)^e g(A)$ , but not every vector is killed by  $\pi(A)g(A)$  since  $\pi(T)g(T)$  is a proper factor of the minimal polynomial  $m_A(T)$ . Set

$$W = \{v \in V : \pi(A)g(A)(v) = 0\},$$

so  $W$  is a proper subspace of  $V$ . Since  $A$  commutes with  $\pi(A)$  and  $g(A)$ ,  $W$  is  $A$ -stable. Assume there is an  $A$ -stable complement to  $W$  in  $V$ . Call it  $W'$ , so  $V = W \oplus W'$ . We will get a contradiction.

The action of  $\pi(A)g(A)$  on  $W'$  is injective: if  $w' \in W'$  and  $\pi(A)g(A)(w') = 0$  then  $w' \in W' \cap W = \{0\}$ . Therefore  $\pi(A)$  is also injective on  $W'$ : if  $\pi(A)(w') = 0$  then applying  $g(A)$  gives  $0 = g(A)\pi(A)(w') = \pi(A)g(A)(w')$ , so  $w' = 0$ . Then  $\pi(A)^e g(A) = \pi(A)^{e-1}(\pi(A)g(A))$  is also injective on  $W'$  since  $\pi(A)$  and  $\pi(A)g(A)$  are injective on  $W'$  and a composite of injective operators is injective. But  $\pi(T)^e g(T) = m_A(T)$  is the minimal polynomial for  $A$ , so  $\pi(A)^e g(A)$  acts as  $O$  on  $V$ , and thus acts as  $O$  on  $W'$  as well. A vector space on which the zero operator acts injectively must be zero, so  $W' = \{0\}$ . Then  $W = V$ , but  $W$  is a proper subspace of  $V$  so we have a contradiction.  $\square$

**Corollary 11.** *If the characteristic polynomial of  $A: V \rightarrow V$  is squarefree then  $A$  is semisimple and  $m_A(T) = \chi_A(T)$ .*

*Proof.* The polynomial  $m_A(T)$  is a factor of  $\chi_A(T)$ , so if  $\chi_A(T)$  is squarefree so is  $m_A(T)$ . Since  $m_A(T)$  and  $\chi_A(T)$  share the same irreducible factors, if  $\chi_A(T)$  is squarefree we must have  $m_A(T) = \chi_A(T)$ ; if  $m_A(T)$  were a proper factor it would be missing an irreducible factor of  $\chi_A(T)$ .  $\square$

**Corollary 12.** *Let  $V$  be a nonzero finite-dimensional vector space.*

- (1) *If the operator  $A: V \rightarrow V$  is semisimple and  $W$  is a proper nonzero  $A$ -stable subspace of  $V$ , the induced linear operators  $A_W: W \rightarrow W$  and  $A_{V/W}: V/W \rightarrow V/W$  are semisimple.*
- (2) *If  $V = W_1 \oplus \cdots \oplus W_k$  and  $A_i: W_i \rightarrow W_i$ , the direct sum  $\bigoplus_{i=1}^k A_i$  acting on  $V$  is semisimple if and only if each  $A_i$  acting on  $W_i$  is semisimple.*
- (3) *If the operator  $A: V \rightarrow V$  is semisimple, there is a direct sum decomposition  $V = W_1 \oplus \cdots \oplus W_k$  where each  $W_i$  is a nonzero  $A$ -stable subspace and  $A$  is a simple operator on each  $W_i$ .*

*Proof.* (1) The minimal polynomials of  $A_W$  and  $A_{V/W}$  divide the minimal polynomial of  $A$ , and any factor of a squarefree polynomial is squarefree.

(2) The minimal polynomial of  $\bigoplus_{i=1}^k A_i$  is the least common multiple of the minimal polynomials of the  $A_i$ 's, and the least common multiple of polynomials is squarefree if and only if each of the polynomials is squarefree (why?).

(3) If  $A$  is a simple operator on  $V$  then the result is trivial. In particular, the case when  $\dim V = 1$  is trivial. If  $A$  does not act as a simple operator on  $V$ , there is a nonzero proper subspace  $W \subset V$  which is  $A$ -stable. Because  $A$  is semisimple, we can write  $V = W \oplus W'$  where  $W'$  is  $A$ -stable (and nonzero). Both  $W$  and  $W'$  have smaller dimension than  $V$ , and by part (1) both  $A_W$  and  $A_{W'}$  are semisimple. Therefore by induction on the dimension of the vector space, we can write  $W$  and  $W'$  as direct sums of nonzero  $A$ -stable subspaces on which  $A$  acts as a simple operator. Combining these direct sum decompositions of  $W$  and  $W'$  gives the desired direct sum decomposition of  $V$ , and  $A$  is the direct sum of its restrictions to these subspaces on which it acts simply.  $\square$

Part 3 says that a semisimple operator is a direct sum of simple operators, and a special case of part 2 says a direct sum of simple operators is semisimple, so semisimplicity is the same as “direct sum of simple operators.”

Since the proof of Theorem 4 applies to semisimple operators (as noted at the start of the proof of Theorem 10), it is natural to ask if the direct sum decomposition of  $V$  in Theorem 4(1) is the “simple” decomposition of  $V$ : does  $A$  act as a simple operator on each  $V_i = \ker \pi_i(A)$ , where the  $\pi_i(T)$ 's are the (monic) irreducible factors of  $m_A(T)$ ? Not necessarily! After all, consider the case of a diagonalizable operator  $A$ . The  $V_i$ 's in Theorem 4 are the eigenspaces of  $A$ , and  $A$  acts on each  $V_i$  as a scaling transformation, which is not simple if  $\dim V_i > 1$ . So if  $A$  is diagonalizable with some eigenspace of dimension larger than 1,  $A$  doesn't act simply on some  $V_i$ . The decomposition  $V = \bigoplus_{i=1}^r V_i$  in Theorem 4 has to be refined further, in general, to get subspaces on which  $A$  is a simple operator.

The converse of part 1 of Corollary 12 is false: if  $A: V \rightarrow V$  is an operator,  $W \subset V$  is  $A$ -stable, and  $A_W$  and  $A_{V/W}$  are semisimple then  $A$  need not be semisimple on  $V$ . Consider  $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  acting on  $V = F^2$  and let  $W = F \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ . Both  $W$  and  $V/W$  are 1-dimensional, so  $A_W$  and  $A_{V/W}$  are semisimple (even simple!), but  $A$  is not semisimple since  $W$  has no  $A$ -stable complement (Example 2 again).

It is natural to ask how we can detect whether a linear operator is simple in terms of its minimal polynomial.

**Theorem 13.** *The following conditions on a linear operator  $A: V \rightarrow V$  are equivalent:*

- (1)  *$A$  is simple:  $A \neq O$  and the only  $A$ -stable subspaces of  $V$  are  $\{0\}$  and  $V$ ,*
- (2) *the minimal polynomial of  $A$  has degree  $\dim V$  and is irreducible in  $F[T]$ ,*
- (3) *the characteristic polynomial of  $A$  is irreducible in  $F[T]$ ,*
- (4)  *$\chi_A(T) = m_A(T)$  is irreducible in  $F[T]$ .*

*Proof.* Since  $m_A(T) | \chi_A(T)$  and  $\chi_A(T)$  has degree  $\dim V$ , the equivalence of the last three conditions is straightforward and left to the reader. We will show conditions 1 and 4 are equivalent.

(4)  $\Rightarrow$  (1): We will show, contrapositively, that an operator  $A$  which is not simple has a reducible characteristic polynomial. When there is a nonzero proper  $A$ -stable subspace  $W \subset V$ ,  $A$  acts on  $W$  and  $V/W$ . Using a basis for  $W$  and the lift to  $V$  of a basis from  $V/W$  as a combined basis for  $V$ , the matrix representation of  $A$  is block diagonal  $\begin{pmatrix} M & \\ 0 & M' \end{pmatrix}$ , where  $M$  is a matrix for  $A$  on  $W$  and  $M'$  is a matrix for  $A$  on  $V/W$ . Then  $\chi_A(T) = \chi_M(T) \chi_{M'}(T)$ , so  $\chi_A(T)$  is reducible in  $F[T]$ .

(1)  $\Rightarrow$  (4): Now we show a simple operator  $A: V \rightarrow V$  has an irreducible characteristic polynomial. Pick any  $v_0 \neq 0$  in  $V$  and set  $W = \{f(A)v_0 : f(T) \in F[T]\}$ . This is an  $A$ -stable subspace and  $W \neq \{0\}$  since  $v_0 \in W$  (use  $f(T) = 1$ ). Therefore, since  $A$  is simple, we must have  $W = V$ . Thus the  $F$ -linear map  $F[T] \rightarrow V$  given by  $f(T) \mapsto f(A)v_0$  is surjective. Since  $\chi_A(T)$  is in the kernel, we get an induced  $F$ -linear map  $F[T]/(\chi_A(T)) \rightarrow V$ . Both sides have the same dimension and the map is onto, so it is an  $F$ -linear isomorphism. In particular, if  $f(A) = O$  then  $f(A)v_0 = 0$  so  $\chi_A(T)|f(T)$ . Hence  $f(A) = O$  if and only if  $\chi_A(T)|f(T)$ .<sup>1</sup> We will show any proper factor of  $\chi_A(T)$  is constant, so  $\chi_A(T)$  is irreducible.

Let  $g(T)$  be a proper factor of  $\chi_A(T)$ , with  $\chi_A(T) = g(T)h(T)$ . Since  $\chi_A(T)$  doesn't divide  $g(T)$ ,  $g(A)v_0 \neq 0$ . Therefore  $\widetilde{W} = \{f(A)g(A)v_0 : f(T) \in F[T]\}$  is a nonzero  $A$ -stable subspace. Because  $A$  is simple,  $\widetilde{W} = V$ . The  $F$ -linear map  $F[T] \rightarrow V$  given by  $f(T) \mapsto f(A)g(A)v_0$  is surjective and  $\chi_A(T)$  is in the kernel, so we get an induced  $F$ -linear map  $F[T]/(\chi_A(T)) \rightarrow V$ . Both sides have the same dimension, so from surjectivity we get injectivity: if  $f(A)g(A)v_0 = 0$  then  $\chi_A(T)|f(T)$ . In particular, since  $h(A)g(A)v_0 = \chi_A(A)v_0 = O(v_0) = 0$ ,  $\chi_A(T)|h(T)$ . Since  $h(T)|\chi_A(T)$  too, we see that  $h(T)$  and  $\chi_A(T)$  have the same degree, so  $g(T)$  must have degree 0.  $\square$

This is *not* saying  $A$  is simple if and only if  $m_A(T)$  is irreducible; the degree condition has to be checked too. Just think about  $\text{id}_V$ , which is not simple if  $\dim V > 1$  and its minimal polynomial is  $T - 1$  (irreducible) but its characteristic polynomial is  $(T - 1)^{\dim V}$  (reducible).

Descriptions of diagonalizable, potentially diagonalizable, semisimple, and simple linear operators in terms of the minimal polynomial are in Table 1.

Property	Minimal Polynomial
Diagonalizable	Splits, distinct roots
Potentially Diagonalizable	Separable
Semisimple	Squarefree
Simple	Irreducible of degree $\dim V$

TABLE 1

A polynomial which splits with distinct roots is separable, and a polynomial which is separable has no repeated irreducible factors, so it is squarefree. Thus diagonalizability implies potential diagonalizability, which implies semisimplicity. Simplicity implies semisimplicity, but simplicity is not related in a uniform way to potential diagonalizability (except over a perfect field, where all irreducibles are separable; there all simple operators are potentially diagonalizable). These implications are not reversible. The 90-degree rotation on  $\mathbf{R}^2$  is potentially diagonalizable and not diagonalizable. Any diagonal matrix  $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$  with distinct diagonal entries is semisimple but not simple.

To give an example of an operator which is semisimple but not potentially diagonalizable is more subtle: we need its minimal polynomial to be squarefree yet not be separable. This is impossible when the scalar field has characteristic 0 or is an algebraically closed field, or more generally is a perfect field. Semisimplicity and potential diagonalizability are the same concept in vector spaces over perfect fields, and over an algebraically closed field

<sup>1</sup>Incidentally, this proves  $m_A(T) = \chi_A(T)$ , although our eventual conclusion that  $\chi_A(T)$  is irreducible already tells us we are going to have  $m_A(T) = \chi_A(T)$  since  $m_A(T)$  is a nonconstant monic factor of  $\chi_A(T)$ .

semisimplicity is the same thing as diagonalizability. (It is common for mathematicians to use the more technical-sounding term semisimple instead of diagonalizable when working over an algebraically closed field, but in that context the terms mean exactly the same thing.) We will construct an operator on a 2-dimensional vector space whose minimal polynomial has degree 2 and is irreducible but not separable, so the operator is simple (and thus semisimple) but not potentially diagonalizable.

**Example 14.** Let  $F$  be a field of characteristic 2 which is not perfect, such as  $\mathbf{F}_2(u)$ . There is an  $\alpha \in F$  such that  $\alpha$  is not a square in  $F$ . The matrix  $A = \begin{pmatrix} 0 & \alpha \\ 1 & 0 \end{pmatrix}$  has characteristic polynomial  $T^2 - \alpha$ . This polynomial is irreducible in  $F[T]$ , since it has degree 2 without roots in  $F$ , so it is squarefree and therefore  $A$  acts semisimply on  $F^2$ . (In fact, the only  $A$ -stable subspaces of  $F^2$  are  $\{0\}$  and  $F^2$ .) The polynomial  $T^2 - \alpha$  has a double root when we pass to a splitting field, since we're in characteristic 2, so  $A$  is not potentially diagonalizable.

If we replace  $F$  with the quadratic extension  $E = F(\sqrt{\alpha})$  then  $A$  does not act semisimply on  $E^2$ . The only eigenvalue of  $A$  is  $\sqrt{\alpha}$ , and the  $\sqrt{\alpha}$ -eigenspace of  $A$  in  $E^2$  is the line spanned by  $\begin{pmatrix} \sqrt{\alpha} \\ 1 \end{pmatrix}$ . This line is an  $A$ -stable subspace with no  $A$ -stable complement in  $E$  since an  $A$ -stable complement would be 1-dimensional and thus spanned by an eigenvector of  $A$ , but all the eigenvectors of  $A$  are scalar multiples of  $\begin{pmatrix} \sqrt{\alpha} \\ 1 \end{pmatrix}$ .

What this example shows us is that semisimplicity need not be preserved under inseparable field extensions. In this respect semisimplicity is not as well-behaved as potential diagonalizability, which is preserved under all field extensions.