# SEMISIMPLICITY 

KEITH CONRAD

A subspace $W$ of an $F$-vector space $V$ always has a complementary subspace: $V=W \oplus W^{\prime}$ for some subspace $W^{\prime}$. This can be seen using bases: extend a basis of $W$ to a basis of $V$ and let $W^{\prime}$ 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: $\mathbf{R}^{n}=W \oplus W^{\prime}$ where $W \perp W^{\prime}$, 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 $W=F v$ 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 $A=\mathrm{id}_{V}$ 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 $A=\left(\begin{array}{ll}1 & 1 \\ 0 & 1\end{array}\right)$ acting on $F^{2}$ and its eigenspace $W=\left\{\binom{x}{0}: x \in F\right\}$. 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 $W=\bigoplus_{i=1}^{r}\left(W \cap E_{\lambda_{i}}\right)$ 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 $W=\sum_{i=1}^{r}\left(W \cap E_{\lambda_{i}}\right)$; 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 $W=\sum_{i=1}^{r}\left(W \cap E_{\lambda_{i}}\right)$. 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 $W_{i}^{\prime}$ be any subspace complement to $W_{i}$ inside $E_{\lambda_{i}}$. Then $W^{\prime}:=\sum_{i=1}^{r} W_{i}^{\prime}=\bigoplus_{i=1}^{r} W_{i}^{\prime}$ is a subspace of $V$ that is $A$-stable (because each $W_{i}^{\prime}$ is $A$-stable) and

$$
W \oplus W^{\prime}=\bigoplus_{i=1}^{r}\left(W_{i} \oplus W_{i}^{\prime}\right)=\bigoplus_{i=1}^{r} E_{\lambda_{i}}=V .
$$

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 $V_{i}=\left\{v \in V: \pi_{i}(A)(v)=0\right\}$.
(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 $W=\bigoplus_{i=1}^{r}\left(W \cap V_{i}\right)$ 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 $A\left(V_{i}\right) \subset V_{i}$ 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 $h_{1}(T), \ldots, h_{r}(T)$ in $F[T]$ such that

$$
\begin{equation*}
1=h_{1}(T)+\cdots+h_{r}(T), \quad h_{i}(T) \equiv 0 \bmod m_{A}(T) / \pi_{i}(T) \tag{1}
\end{equation*}
$$

Once these polynomials are found, $\pi_{i}(T) h_{i}(T)$ is divisible by $m_{A}(T)$ for all $i$, so $\pi_{i}(A) h_{i}(A)=$ $O$. Then replacing $T$ with the operator $A$ in (1) and applying all operators to any $v \in V$ gives

$$
v=h_{1}(A)(v)+\cdots+h_{r}(A)(v), \quad \pi_{i}(A) h_{i}(A)(v)=0 .
$$

The second equation tells us $h_{i}(A)(v) \in V_{i}$, so the first equation shows $V=V_{1}+\cdots+V_{r}$. To show this sum is direct, suppose

$$
\begin{equation*}
v_{1}+\cdots+v_{r}=0 \tag{2}
\end{equation*}
$$

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 $j \neq i, h_{i}(A)\left(v_{j}\right)=0$ for $j \neq i$ (look at the definition of $V_{j}$ ). Therefore $h_{i}(A)\left(v_{i}\right)=0$. Also $\pi_{i}(A)\left(v_{i}\right)=0$ by the definition of $V_{i}$, so $h_{j}(A)\left(v_{i}\right)=0$ for $j \neq i$. Thus $\operatorname{id}_{V}=h_{i}(A)+\sum_{j \neq i} h_{j}(A)$ 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 :

$$
1=g_{1}(T) f_{1}(T)+\cdots+g_{r}(T) f_{r}(T)
$$

Use $h_{i}(T)=g_{i}(T) f_{i}(T)$.
(2) We will show $W=\sum_{i=1}^{r}\left(W \cap V_{i}\right)$. 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 $A\left(W_{i}\right) \subset W_{i}, W_{i}$ 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 $W_{i}^{\prime}$ of $V_{i}$ such that $V_{i}=W_{i} \oplus W_{i}^{\prime}$. Since $\pi_{i}(T)$ kills $V_{i}, V_{i}$ is an $F[T] /\left(\pi_{i}\right)$-module and $W_{i}$ is an $F[T] /\left(\pi_{i}\right)$-submodule. Now $F[T] /\left(\pi_{i}\right)$ is a field, so $V_{i}$ is a vector space over $F[T] /\left(\pi_{i}\right)$ and $W_{i}$ is a subspace over this field. Set $W_{i}^{\prime}$ to be any complementary subspace to $W_{i}$ inside $V_{i}$ as $F[T] /\left(\pi_{i}\right)$-vector spaces. (When $\operatorname{det} \pi_{i}>1$, this is a stronger condition than being a complementary subspace in $V_{i}$ as $F$-vector spaces.) Since $W_{i}^{\prime}$ is an $F[T] /\left(\pi_{i}\right)$ submodule of $V_{i}$, it is an $F$-vector space and $A$-stable, so we are done: $W^{\prime}=\sum_{i=1}^{r} W_{i}^{\prime}$ is an $A$-stable complement to $W$ in $V$.

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 $V=W \oplus W^{\prime}$ for some subspace $W^{\prime}$ such that $A\left(W^{\prime}\right) \subset W^{\prime}$.

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 $\left.W_{i}\right)$. 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 $W^{\prime}$, so $V=W \oplus W^{\prime}$. We will get a contradiction.

The action of $\pi(A) g(A)$ on $W^{\prime}$ is injective: if $w^{\prime} \in W^{\prime}$ and $\pi(A) g(A)\left(w^{\prime}\right)=0$ then $w^{\prime} \in$ $W^{\prime} \cap W=\{0\}$. Therefore $\pi(A)$ is also injective on $W^{\prime}$ : if $\pi(A)\left(w^{\prime}\right)=0$ then applying $g(A)$ gives $0=g(A) \pi(A)\left(w^{\prime}\right)=\pi(A) g(A)\left(w^{\prime}\right)$, so $w^{\prime}=0$. Then $\pi(A)^{e} g(A)=\pi(A)^{e-1}(\pi(A) g(A))$ is also injective on $W^{\prime}$ since $\pi(A)$ and $\pi(A) g(A)$ are injective on $W^{\prime}$ 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 $W^{\prime}$ as well. A vector space on which the zero operator acts injectively must be zero, so $W^{\prime}=\{0\}$. Then $W=V$, but $W$ is a proper subspace of $V$ so we have a contradiction.

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 $\chi_{A}(T)$.

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 $\operatorname{dim} V=1$ 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 $V=W \oplus W^{\prime}$ where $W^{\prime}$ is $A$-stable (and nonzero). Both $W$ and $W^{\prime}$ have smaller dimension than $V$, and by part (1) both $A_{W}$ and $A_{W^{\prime}}$ are semisimple. Therefore by induction on the dimension of the vector space, we can write $W$ and $W^{\prime}$ as direct sums of nonzero $A$-stable subspaces on which $A$ acts as a simple operator. Combining these direct sum decompositions of $W$ and $W^{\prime}$ 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.

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 $V_{i}=\operatorname{ker} \pi_{i}(A)$, 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 $\operatorname{dim} V_{i}>1$. 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 $A=\left(\begin{array}{ll}1 & 1 \\ 0 & 1\end{array}\right)$ acting on $V=F^{2}$ and let $W=F\binom{1}{0}$. 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 $\operatorname{dim} V$ 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 $m_{A}(T) \mid \chi_{A}(T)$ and $\chi_{A}(T)$ has degree $\operatorname{dim} V$, 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 upper-triangular $\left(\begin{array}{cc}M & * \\ O & M^{\prime}\end{array}\right)$, where $M$ is a matrix for $A$ on $W$ and $M^{\prime}$ is a matrix for $A$ on $V / W$. Then $\chi_{A}(T)=\chi_{M}(T) \chi_{M^{\prime}}(T)$, 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 $W=\left\{f(A) v_{0}: f(T) \in F[T]\right\}$. 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 $F[T] /\left(\chi_{A}(T)\right) \rightarrow V$. 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 $\chi_{A}(T) \mid f(T)$. Hence $f(A)=O$ if and only if $\chi_{A}(T) \mid f(T) .{ }^{1}$ 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 $\widetilde{W}=\left\{f(A) g(A) v_{0}: f(T) \in F[T]\right\}$ 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 $F[T] /\left(\chi_{A}(T)\right) \rightarrow V$. Both sides have the same dimension, so from surjectivity we get injectivity: if $f(A) g(A) v_{0}=0$ then $\chi_{A}(T) \mid f(T)$. In particular, since $h(A) g(A) v_{0}=$ $\chi_{A}(A) v_{0}=O\left(v_{0}\right)=0, \chi_{A}(T) \mid h(T)$. Since $h(T) \mid \chi_{A}(T)$ too, we see that $h(T)$ and $\chi_{A}(T)$ have the same degree, so $g(T)$ must have degree 0 .

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 $\operatorname{id}_{V}$, which is not simple if $\operatorname{dim} V>1$ and its minimal polynomial is $T-1$ (irreducible) but its characteristic polynomial is $(T-1)^{\operatorname{dim} V}$ (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 <br> Semisimple | Squareflee |
| Simple | Irreducible of degree $\operatorname{dim} V$ |
| 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 $\left(\begin{array}{cc}a & 0 \\ 0 & b\end{array}\right)$ 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

[^0]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 $A=\left(\begin{array}{ll}0 & \alpha \\ 1 & 0\end{array}\right)$ 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 $\binom{\sqrt{\alpha}}{1}$. 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 $\binom{\sqrt{\alpha}}{1}$.

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.


[^0]:    ${ }^{1}$ 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 $\chi_{A}(T)$.

