MATH 210A, FALL 2017
HW 9 SOLUTIONS
WRITTEN BY DAN DORE
(If you find any errors, please email ddore@stanford.edu)

Let V be a vector space over a field $\mathbf{F}$, and let $\omega\colon V \times V \to \mathbf{F}$ be an alternating form. An ω-*symplectic basis* is an ordered basis $a_1, b_1, a_2, b_2, \dots, a_n, b_n$ for V with the property that

$$\omega(a_i, b_i) = 1 \quad \text{for all } i$$

$$\omega(a_i, a_j) = \omega(a_i, b_j) = \omega(b_i, a_j) = \omega(b_i, b_j) = 0 \text{ if } i \neq j$$

Question 1. Suppose that ω is a nondegenerate alternating form over an arbitrary[1] field $\mathbf{F}$. Prove there exists an ω-symplectic basis.

Solution. Note that in particular, we are showing that any vector space which admits an alternating non-degenerate form has even dimension $2n$. We will show by induction on n that a vector space of dimension $2n$ with a non-degenerate alternating form admits a symplectic basis and that a vector space of dimension $2n+1$ does not admit a non-degenerate symplectic form. The base case is $n = 0$. When V has dimension 0 the claim is vacuously true. When $V = \mathbf{F} \cdot e$ has dimension 1, there cannot be a non-degenerate alternating form ω on V: $\omega(xe, ye) = xy\omega(e, e) = 0$ for any $x, y \in \mathbf{F}$.

Now, both inductive steps will rest on the following lemma:

Lemma 1. Let V be a vector space with a non-degenerate alternating form ω on V. If $V_1 \subseteq V$ is a two-dimensional subspace with basis vectors e, f with $\omega(e, f) = 1$, then if $V_2 := V_1^{\perp} = \{v \in V \mid \omega(v, V_1) = 0\}$ is the orthogonal complement of V_1 in V with respect to ω, we have $V = V_1 \oplus V_2$ and furthermore $\omega|_{V_2}$ is alternating and non-degenerate.

Before we prove the lemma, let's see why it suffices for both inductive steps. For arbitrary $a \in V$, there exists $b' \in V$ with $\omega(a, b') \neq 0$ by nondegeneracy. Taking $b = \frac{1}{\omega(a,b)} b'$ we have $\omega(a, b) = 1$. In particular a and b are linearly independent (because otherwise $\omega(a, b) = \omega(a, ca) = c\omega(a, a) = 0$). So let V_1 be the space of a, b. Thus, we may apply the lemma. In particular it implies $\dim V_2 = \dim V - 2$. If the dimension of V is odd, so is the dimension of V_2, but the lemma shows that $\omega|_{V_2}$ is an alternating non-degenerate form on V_2. By induction, we know that this is impossible.

If the dimension of V is even, so is the dimension of V_2, so we may find a symplectic basis $a_2, b_2, \dots, a_n, b_n$ for V_2. Then letting $a_1 = a, b_1 = b$, we can see that $a_1, b_1, a_2, b_2, \dots, a_n, b_n$ is a symplectic basis since $\omega(a_1, b_1) = 1$, $a_2, b_2, \dots, a_n, b_n$ is a symplectic basis for V_2, and a_1, b_1 live in the orthogonal complement to V_2.

Now, we must prove the lemma:

Proof. First, note that $V_1 \cap V_2 = 0$. To see this, let $ce + df \in V_1$ with $c, d \in \mathbf{F}$. If this is in V_2, then we have $0 = \omega(ce + df, e) = d\omega(f, e) = -d$ and $0 = \omega(ce + df, f) = c\omega(e, f) = c$, so $c = 0$ and $d = 0$.

Now, we need to show that $V = V_1 + V_2$. To do this, since $V_1 \cap V_2 = 0$, it suffices to show that $\dim V_2 = \dim V - 2$. Now, the bilinear form ω induces a map $\widetilde{\omega}\colon V \to V^{\vee}$ by sending $v \in V$ to the map

[1] Note we do not need to assume anything about which elements are squares, nor anything about $\operatorname{char} \mathbf{F}$.

$w \mapsto \omega(v, w)$. Non-degeneracy of ω means exactly that $\widetilde{\omega}$ is injective: if $\omega(v, w) = 0$ for all $w \in V$, then $v = 0$. Since $V, V^\vee$ are vector spaces of the same finite dimension, this implies that $\widetilde{\omega}$ is an isomorphism.

V_2 exactly consists of the v such that $\widetilde{\omega}(v)|_{V_1} = 0$. But the map from $V^\vee$ to $(V_1)^\vee$ sending φ to $\varphi|_{V_1}$ is a surjection onto the two-dimensional vector space $(V_1)^\vee$, so its kernel has codimension 2 in $V^\vee$. Therefore, V_2 has codimension 2 in V, so we have shown $V = V_1 \oplus V_2$.

Now, we need to show that $\omega|_{V_2}$ is alternating and non-degenerate. The fact that it is alternating is obvious: for $v \in V_2$, $\omega|_{V_2}(v, v) = \omega(v, v) = 0$. To see that it is non-degenerate, fix some $v \in V_2$. We need to find some $w \in V_2$ with $\omega|_{V_2}(v, w) = \omega(v, w) \neq 0$. Since ω is non-degenerate, we may pick some $w_0 \in V$ with $\omega(v, w_0) \neq 0$. Since $V = V_1 \oplus V_2$, we may uniquely write $w_0 = w_1 + w_2$ with $w_i \in V_i$. Then we have $\omega(v, w_0) = \omega(v, w_1) + \omega(v, w_2) = \omega(v, w_2)$, since $w_1 \in V_1$ and V_2 is ω-orthogonal to V_1. Thus, $\omega(v, w_2) \neq 0$, so we are done. □

Question 2. Let V be a $2n$-dimensional vector space over $\mathbf{F}$. Recall that $V^\vee$ denotes the dual vector space $V^\vee = \mathrm{Hom}_{\mathbf{F}}(V, \mathbf{F})$.

Let $\omega \colon V \times V \to \mathbf{F}$ be an alternating form. We can view ω as an element of $\bigwedge^2(V^\vee)$. (make sure you understand how this correspondence works)

Is it true that ω is nondegenerate as a bilinear form if and only if $\omega \wedge \cdots \wedge \omega \in \bigwedge^{2n}(V^\vee)$ is nonzero?

Solution. First, let's make the correspondence between the space of alternating forms on V and $\bigwedge^2(V^\vee)$ precise.

Proposition 2. For a vector space $V \simeq \mathbf{F}^{2n}$, there is a natural linear isomorphism $\omega \mapsto \mathrm{ev}_\omega$ between $\bigwedge^2 V^\vee$ and the vector space of alternating bilinear forms on V.

Proof. Note that the space of skew-symmetric bilinear forms on V is canonically isomorphic to $(\bigwedge^2 V)^\vee$: the universal property of exterior powers says exactly that a linear map from $\bigwedge^2 V$ to $\mathbf{R}$ is the same thing as a skew-symmetric bilinear form on V. So we are defining a map from $\bigwedge^2(V^\vee)$ to $(\bigwedge^2 V)^\vee$. We define this by mapping $\varphi \wedge \psi$ to the bilinear form $\mathrm{ev}_{\varphi\wedge\psi} \colon (v, w) \mapsto \varphi(v)\psi(w) - \psi(v)\varphi(w)$. Since this map is clearly linear in each of v, w, φ, ψ, this at least defines a map from $V^\vee \otimes V^\vee$ to $(V \otimes V)^\vee$. Since $\mathrm{ev}_{\varphi\wedge\psi} = -\mathrm{ev}_{\psi\wedge\varphi}$, it factors through the canonical projection $V^\vee \otimes V^\vee \to \bigwedge^2(V^\vee)$, so it gives us a map $\bigwedge^2(V^\vee)$ to $(V \otimes V)^\vee$. Finally, since $\mathrm{ev}_{\varphi\wedge\psi}(v, v) = \varphi(v)\psi(v) - \varphi(v)\psi(v) = 0$, the image lands inside the subspace of alternating forms $(V \wedge V)^\vee \subseteq (V \otimes V)^\vee$. Note that this definition makes it clear that $\mathrm{ev}_\bullet$ is functorial in V, i.e. that if $T \colon V \to W$ is a linear map, then

$$\begin{aligned}
\mathrm{ev}_{T^*(\varphi\wedge\psi)}(v_1, v_2) &= \mathrm{ev}_{(T^*\varphi\wedge T^*\psi)}(v_1, v_2) \\
&= \varphi(T(v_1))\psi(T(v_2)) - \psi(T(v_2))\varphi(T(v_1)) \\
&= \mathrm{ev}_{\varphi,\psi}(T(v_1), T(v_2)) \\
&= (T^*\mathrm{ev}_{\varphi,\psi})(v_1, v_2)
\end{aligned}$$

We can compute what this is explicitly in a basis (note that the above construction was basis-independent!) $v_1, \ldots, v_{2n}$ of V, with associated dual basis $v^1, \ldots, v^{2n}$ of $V^\vee$ (defined by $v^i(v_j) = \delta^i_j$). For $\omega \in \bigwedge^2(V^\vee)$, we may write $\omega = \sum_{i<j} a_{ij} v^i \wedge v^j$, $v = \sum_i b_i v_i$, and $w = \sum_j c_j v_j$. Then we have

$$\mathrm{ev}_\omega(v, w) = \sum_{i<j} a_{ij}(b_i c_j - b_j c_i) \tag{1}$$

We can check explicitly that this is alternating: if $b_i = c_i$, this is $\sum_{i<j} a_{ij}(b_i b_j - b_j b_i) = 0$. To see that the map is an isomorphism, note that for $i < j$, $\mathrm{ev}_\omega(v_i, v_j) = a_{ij}$. Thus, if $\mathrm{ev}_\omega = 0$, we have $a_{ij} = 0$ for all $i < j$, so $\omega = 0$. This shows that $\mathrm{ev}_\bullet$ is injective, and since $\bigwedge^2 V$ and $(\bigwedge^2 V^\vee)^\vee$ both have dimension $\binom{2n}{2}$, we conclude that $\mathrm{ev}_\bullet$ is an isomorphism. $\square$

We can show one direction right away: if $\omega \wedge \cdots \wedge \omega \neq 0$ in $\bigwedge^{2n}(V^\vee)$, then ev_ω is non-degenerate. Indeed, assume that ev_ω is degenerate so that there exists some $v \in V$ with $\mathrm{ev}_\omega(v, w) = 0$ for all $w \in V$. Let $V_1 = \mathbf{F} \cdot v$, and let $W = V/V_1$. Then also $\mathrm{ev}_\omega(w, v) = -\mathrm{ev}_\omega(v, w) = 0$, so ev_ω descends to an alternating form on W. By functoriality of the map $\omega \mapsto \mathrm{ev}_\omega$, this means that ω is in the image of the natural inclusion $\bigwedge^2(W^\vee) \hookrightarrow \bigwedge^2(V^\vee)$. Thus, $\omega \wedge \cdots \wedge \omega \in \bigwedge^{2n}(V^\vee)$ is in the image of the natural inclusion of $\bigwedge^{2n}(W^\vee)$. But this space is 0 since W has dimension $2n - 1$.

We can also work explicitly in a basis: assume that $\mathrm{ev}_\omega(v, w) = 0$ for all $w \in V$. Then we can choose a basis $v_1, \ldots, v_{2n}$ of V with $v_1 = v$. Let $\varphi^1, \ldots, \varphi^{2n}$ be the dual basis of $V^\vee$, i.e. $\varphi^i(v_j) = \delta^i_j$. Write $\omega = \sum_{i<j} a_{ij} \varphi^i \wedge \varphi^j$. Then for all $j = 1, \ldots, 2n$, we have $0 = \mathrm{ev}_\omega(v_1, v_j) = a_{1j}$. Thus, φ^1 does not occur in the expression for ω, so ω is in $\bigwedge^2 V'$, where V' is the span of $\varphi^2, \ldots, \varphi^{2n}$. Thus, $\wedge^n(\omega)$ is in $\bigwedge^{2n} V' = 0$, so $\wedge^n(\omega) = 0$.

Now, assume that ev_ω is non-degenerate as a bilinear form. By Question 1, we may pick a symplectic basis $a_1, b_1, \ldots, a_n, b_n$ for V, i.e. $\mathrm{ev}_\omega(a_i, b_i) = 1$ and $\mathrm{ev}_\omega(a_i, a_j) = \mathrm{ev}_\omega(b_i, b_j) = \mathrm{ev}_\omega(a_i, b_j) = 0$ for all $i \neq j$. If we let $a^1, b^1, \ldots, a^n, b^n$ be the dual basis for $V^\vee$ and express ω in terms of this basis, Equation (1) shows that $\omega = a^1 \wedge b^1 + a^2 \wedge b^2 + \cdots + a^n \wedge b^n$.

We may compute explicitly that $\omega \wedge \cdots \wedge \omega = n!\left(a^1 \wedge b^1 \wedge a^2 \wedge \cdots \wedge a^n \wedge b^n\right) \in \bigwedge^{2n}(V^\vee)$: this is done in the solution to Question 1 on HW8 (while the computation there is stated in the case $\mathbf{F} = \mathbf{R}$, this assumption is only used to conclude that $n! \neq 0$). Thus, we see that (because $n! \neq 0$ in a field $\mathbf{F}$ iff $\mathrm{char}(\mathbf{F}) > n$):

Proposition 3. If $\omega \in \bigwedge^2(V^\vee)$ for a vector space V of dimension $2n$ over a field $\mathbf{F}$, $\omega \wedge \cdots \wedge \omega \neq 0$ iff ev_ω is non-degenerate and $\mathrm{char}(\mathbf{F}) > n$.

Question 3. Let $\mathbf{F}_q$ be a finite field of order q and characteristic $p \neq 2$, and let V be a 2-dimensional vector space over F_q. Let us say a "*quasi-definite*[2] form" is a symmetric bilinear form $\omega \colon V \times V \to \mathbf{F}_q$ with the property that $\omega(v, v) \neq 0$ for all $v \neq 0 \in V$.

(a) How many different isomorphism classes of quasi-definite forms are there?
Please begin your answer by giving the number of isomorphism classes, and then giving one clear representative of each isomorphism class (and then prove your answer is correct, of course).
Note that the answer[3] may depend on properties of q or F_q.

(b) (Optional) Same question, but when $q = 2^k$.

Solution. (a) We will prove the following:

Proposition 4. If $\mathbf{F}_q$ is a finite field of order q and characteristic $p \neq 2$, V is a 2-dimensional vector space over $\mathbf{F}_q$, and ω is a quasi-definite form on V, there is a basis e_1, e_2 of V such that

[2] "quasi-definite" isn't an official term; I made it up because it's kind of like positive-definite, except of course "positive" doesn't mean anything in $\mathbf{F}_q$

[3] but of course the number is finite, because there are only finitely many *set functions* $V \times V \to \mathbf{F}_q$

$\omega(e_1, e_1) = 1, \omega(e_1, e_2) = \omega(e_2, e_1) = 0$, and $\omega(e_2, e_2) = -d$ where $d \in \mathbf{F}_q^\times$ is not a square. Furthermore, the bilinear forms arising from any two choices of non-square d are isomorphic.

To see the second statement, note that by replacing e_2 with ae_2 for $a \in \mathbf{F}_q$, we replace d with $a^2 d$ and otherwise keep the same form. Thus, only the class of d in $\mathbf{F}_q^\times/(\mathbf{F}_q^\times)^2$ matters. But $\mathbf{F}_q^\times$ is a cyclic group,[4] isomorphic to $\mathbf{Z}/(q-1)\mathbf{Z}$, so as $2 \mid (q-1)$, $\mathbf{F}_q^\times/(\mathbf{F}_q^\times)^2 \simeq \mathbf{Z}/2\mathbf{Z}$, so the requirement that d is not a square uniquely determines its class in $\mathbf{F}_q^\times/(\mathbf{F}_q^\times)^2$.

Proof. Let $v_1 \neq 0 \in V$ be arbitrary and let V_2 be the orthogonal complement $V_2 = \{v \in V \mid \omega(v_1, v) = 0\}$. Since $\omega(v_1, v_1) \neq 0$, $v_1 \notin V_2$. As ω is non-degenerate, the proof of Lemma 1 carries through to show that $\dim V_2 = 1$, so we can choose some $v_2 \in V_2$ such that $\{v_1, v_2\}$ is a basis for V. Let $\omega(v_1, v_1) = d_1$, $\omega(v_2, v_2) = d_2$. By replacing v_i with $a_i v_i$, we can change the d_i by squares, so only the classes of d_1, d_2 in $\mathbf{F}_q^\times/(\mathbf{F}_q^\times)^2$ matter. Then, the condition that $\omega(v, v) \neq 0$ for all v says exactly that there are no solutions with $a, b \in \mathbf{F}_q$ to the equation:

$$0 = \omega(av_1 + bv_2, av_1 + bv_2) = a^2 d_1 + b^2 d_2$$

Rearranging and dividing by b^2 and d_1, this says that $-d_2/d_1$ is not a square in $\mathbf{F}_q$. Thus, since $\mathbf{F}_q^\times/(\mathbf{F}_q^\times)^2 \simeq \mathbf{Z}/2$, exactly one of d_1 and $-d_2$ is a square. If d_1 is a square, we can arrange that $d_1 = 1$, and this suffices to prove the proposition. Now, if -1 is a square in $\mathbf{F}_q$, we could conclude that d_2 is a square and switch the roles of d_1 and d_2 to conclude as above. In general, we need to prove that if $\omega(\cdot, \cdot)$ is a quasi-definite symmetric bilinear form on a two-dimensional vector space V over $\mathbf{F}_q$, then there is some $v \in V$ such that $\omega(v, v)$ is a square. Since scaling V by $a \in \mathbf{F}_q$ changes $\omega(v, v)$ by a^2, we see that this is equivalent to saying that there is some $v \in V$ with $\omega(v, v) = 1$. In order to prove this, we will actually prove a stronger statement:

Lemma 5. If ω is a quasi-definite symmetric bilinear form on a vector space V of dimension 2 over $\mathbf{F}_q$ with characteristic $p \neq 2$, then the map $Q_\omega \colon V \to \mathbf{F}_q$ defined by $v \mapsto \omega(v, v)$ is surjective[5].

Proof. As above, we may choose a basis v_1, v_2 for V such that $\omega(v_1, v_2) = 0$, $\omega(v_1, v_1) = d_1$, and $\omega(v_2, v_2) = d_2$. By replacing ω by $\omega' = d_1^{-1}\omega$, we may assume that $d_1 = 1$ (if $Q_{\omega'}$ is surjective, then $Q_\omega = d_1 Q_{\omega'}$ is surjective, as multiplication by the unit d_1 is surjective). Thus, we may assume ω is of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -d \end{smallmatrix}\right)$ with d non-square. Then $Q_\omega(av_1 + bv_2) = a^2 - db^2$.

Since $Q_\omega(xv) = x^2 Q_\omega(v)$, Q_ω is surjective iff it is surjective onto $\mathbf{F}_q^\times/(\mathbf{F}_q^\times)^2$. Since we are assuming $Q_\omega(av_1 + bv_2) = a^2 - db^2$, we see that $Q_\omega(v_1) = 1$, which is a square. Thus, we must show that the image of Q_ω in $\mathbf{F}_q^\times$ is not equal to $(\mathbf{F}_q^\times)^2$. Assume for the sake of contradiction that this is the case. Then, in particular, $-d = Q_\omega(av_1 + bv_2)$ is a square c^2, so we have $Q_\omega(av_1 + bv_2) = a^2 + (cb)^2$. Then since $c \neq 0$, if $b' \in \mathbf{F}_q^\times$, we may take $b = b'c^{-1}$, so $Q_\omega(av_1 + bv_2) = a^2 + (b')^2$, so for any $a, b' \in \mathbf{F}_q^\times$, $a^2 + (b')^2$ is a square. Since $av_1 + bv_2 \neq 0$, $a^2 + (b')^2$ is a *non-zero* square by quasi-definiteness of ω.

[4]More generally, any finite subgroup of the multiplicative group of a field is cyclic. This is because for any n, the number of solutions in a field $\mathbf{F}$ of the equation $x^n = 1$ is at most n. Thus, if $G \subseteq \mathbf{F}^\times$ is a subgroup such that every element of G has order dividing n, then $|G| \leq n$. Now, if $G \subseteq \mathbf{F}^\times$ is finite, by the structure theorem for finitely generated abelian groups, $G = \mathbf{Z}/n_1 \oplus \mathbf{Z}/n_2 \oplus \cdots \oplus \mathbf{Z}/n_k$ for $n_1 \mid n_2 \mid \cdots \mid n_k$. Then every element of the subgroup $\mathbf{Z}/n_1 \oplus \mathbf{Z}/n_2$ has order dividing n_2, but there are $n_1 \cdot n_2$ elements, so $n_1 = 1$ by the above discussion. Then we can induct on k to conclude.

[5]This is the *quadratic form* associated to ω

In particular, $2 = 1^2 + 1^2$ is a square x^2, so $3 = 1^2 + x^2$ is a square, and continuing on like this we see that $1 + 1 + \cdots + 1 \in \mathbf{F}_q$ is a non-zero square for any number of 1's. However, taking p 1's, this sum is 0, which gives the desired contradiction. $\square$

As shown above, this suffices for the proof of the problem. $\square$

As a side note: we may interpret the surjectivity result in Lemma 5 a little bit differently, using the arithmetic of field extensions of finite fields. Consider the quadratic field extension $\mathbf{F}_{q^2}/\mathbf{F}_q$ defined by adjoining a square root of d to $\mathbf{F}_q$ (as any two non-squares in $\mathbf{F}_q$ differ by multiplication by a square, there is a unique such extension). We know that $\mathbf{F}_{q^2}^\times$ is cyclic of order $q^2 - 1 = (q-1)(q+1)$, and $\mathbf{F}_q^\times$ is its unique subgroup of order $q-1$. Thus, $\mathbf{F}_q^\times = \{x^{q+1} \mid x \in \mathbf{F}_{q^2}\}$, i.e. the map $x \mapsto x^{q+1}$ gives a surjection from $\mathbf{F}_{q^2}$ to $\mathbf{F}_q$.

An element of $\mathbf{F}_{q^2}$ may be written uniquely in the form $a + b\sqrt{d}$, and $Q_\omega(av_1 + bv_2) = a^2 - db^2 = (a + b\sqrt{d})(a - b\sqrt{d})$. Thus, if we identify V with the two-dimensional vector space $\mathbf{F}_{q^2}$ by sending v_1 to 1 and v_2 to d, Q_ω becomes the map $x \mapsto x\overline{x}$, where $\overline{a + b\sqrt{d}} = a - b\sqrt{d}$. The map $x \mapsto \overline{x}$ is unique non-trivial field automorphism in the Galois group of $\mathbf{F}_{q^2}$ over $\mathbf{F}_q$, since it exchanges the two roots of the polynomial $X^2 - d$. Thus, we may identify Q_ω with the *norm* $N(x) = x\overline{x}$, and we want to show that this is surjective. In order to do so, we will show that $N(x) = x^{q+1}$, identifying Q_ω with the surjective map $x \mapsto x^{q+1}$ from $\mathbf{F}_{q^2}$ to $\mathbf{F}_q$. This amounts to verifying that $x^q = \overline{x}$.

Since $\mathbf{F}_{q^2}$ has characteristic p and $q = p^k$ for some k, we have the identity $(x+y)^q = x^q + y^q$: when we take the binomial expansion, all other coefficients are divisible by p. Thus, $(a+b\sqrt{d})^q = a^q + b^q(\sqrt{d})^q$. Since $\mathbf{F}_q^\times$ is cyclic of order $q-1$ and $a, b \in \mathbf{F}_q$, $a^{q-1} = b^{q-1} = 1$, so we have:

$$(a + b\sqrt{d})^q = a + b(\sqrt{d})^q$$

Thus, we must show that $(\sqrt{d})^q = -\sqrt{d}$. Since $\sqrt{d} \in \mathbf{F}_{q^2}^\times \setminus \mathbf{F}_q^\times$, we know that $(\sqrt{d})^{q^2-1} = 1$ but $(\sqrt{d})^{q-1} \neq 1$, as $\mathbf{F}_q^\times$ is the subgroup of $\mathbf{F}_{q^2}^\times$ of elements with order dividing $q-1$. Thus, $(\sqrt{d})^q \neq \sqrt{d}$. This shows that the map $x \mapsto x^q$ is a field automorphism which is non-trivial, so it must coincide with $x \mapsto \overline{x}$ as the Galois group of the quadratic extension $\mathbf{F}_{q^2}/\mathbf{F}_q$ is cyclic of degree 2. We can also see this directly:

We have $(\sqrt{d})^2 = d$, so $((\sqrt{d})^q)^2 = ((\sqrt{d})^2)^q = d^q = d$, since $d \in \mathbf{F}_q^\times$. Thus, $(\sqrt{d})^q$ is a solution in $\mathbf{F}_{q^2}$ of the polynomial $X^2 - d$. This polynomial factors as $(X - \sqrt{d})(X + \sqrt{d})$, so we must have $(\sqrt{d})^q = \pm\sqrt{d}$. But we know $(\sqrt{d})^q \neq \sqrt{d}$, so we must have $(\sqrt{d})^q = -\sqrt{d}$.

(b) Let $q = 2^k$. Then we will show there are no quasi-definite forms ω on a two-dimensional vector space V over $\mathbf{F}_q$. Indeed, assume ω is such a form. Then pick some $v_1 \in V$. Let $V_1 = \mathbf{F}_q \cdot v_1$ and V_2 be its ω-orthogonal complement in V. Then, as in the previous part, the fact that ω is non-degenerate and that $\omega(v_1, v_1) \neq 0$ implies that $V = V_1 \oplus V_2$. Thus, we have a basis $\{v_1, v_2\}$ such that $\omega(v_1, v_2) = 0$, $\omega(v_1, v_1) = d_1$, and $\omega(v_2, v_2) = d_2$. Now, if we replace v_1 with av_1 for $a \in \mathbf{F}_q$, we can change d_1 to $a^2 d_1$ while keeping the form otherwise the same. Thus, we may change d_1 and d_2 by multiplying by arbitrary squares. However, since $q = 2^k$, $\mathbf{F}_q^\times \simeq \mathbf{Z}/(2k-1)\mathbf{Z}$, and this is a cyclic group of odd order. Therefore, the operation $x \mapsto x^2$ is an isomorphism, so in particular, every element of $\mathbf{F}_q^\times$ is a square. (Alternatively, since $\mathbf{F}_q$ has characteristic 2, $(x+y)^2 = x^2 + 2xy + y^2 = x^2 + y^2$, so squaring is a homomorphism of fields and is therefore an automorphism). Thus, we may arrange for $d_1 = d_2 = 1$. Now, we have $\omega(av_1 + bv_2, av_1 + bv_2) = a^2 + b^2$. But taking $a = b$, this is $2a^2 = 0$, so ω is not quasi-definite.

What about the norm of a degree-two field extension? If $\mathbf{F}_q$ has characteristic 2, there is still a unique quadratic extension $\mathbf{F}_{q^2}$ and the norm map $x \mapsto N(x) = x \cdot x^q$ is a surjective homomorphism from $\mathbf{F}_{q^2}^\times$ to $\mathbf{F}_q^\times$. However, this quadratic form is not of the form $Q_\omega(v) = \omega(v, v)$ for any symmetric bilinear form ω, unlike the case when the characteristic is not 2.

We know that every ideal in $\mathbf{R}[x]$ is principal (generated by one element). How about $\mathbf{Z}[x]$?

Question 4. Let $R = \mathbf{Z}[x]$, and consider an ideal $I \subset \mathbf{Z}[x]$. Prove that I is generated by finitely many elements. Is there an upper bound on how many generators we need? (i.e. is every ideal gen by 2 elements? or by 5 elements? etc.)

Solution. Since $\mathbf{Z}$ is a principal ideal domain, in particular it is a noetherian ring: every ideal is generated by a single element. Then, our result follows from:

Theorem 6 (Hilbert Basis Theorem)**.** If R is a noetherian ring, then the ring $R[x]$ is also noetherian.

Thus, $\mathbf{Z}[x]$ is noetherian, i.e. every ideal is finitely generated. We'll walk through the proof of this theorem in the case $R = \mathbf{Z}$ (but it easily generalizes to arbitrary noetherian R).

Proof. Let $I \subseteq \mathbf{Z}[x]$ be an ideal. For each degree k, let I_k be the set of leading coefficients of all elements of I of degree k, i.e. $I_k = \{n \in \mathbf{Z} \mid \exists p(x) \in I, p(x) = nx^k + a_{k-1}x^{k-1} + \cdots + a_0\}$. This is an ideal of $\mathbf{Z}$: To see this, let $n, m \in I_k$, so there are $p(x), q(x) \in I$ with $p(x) = nx^k + a_{k-1}x^{k-1} + \cdots + a_0, q(x) = mx^k + b_{k-1}x^{k-1} + \cdots + b_0$. Then since $p(x), q(x) \in I$, we have for any $d \in \mathbf{Z}$, $(n + dm)x^k + c_{k-1}x^{k-1} + \cdots + c_0 = p(x) + dq(x) \in I$. Thus, $n + dm \in I_k$ for any $d \in \mathbf{Z}$, so I_k is an ideal. Now, $I_k \subseteq I_{k+1}$ for any k, since if $p(x) = nx^k + a_{k-1}x^{k-1} + \cdots + a_0 \in I$, then $xp(x) = nx^{k+1} + a_{k-1}x^k + \cdots + a_0x \in I$ as well, so $n \in I_k$ implies $n \in I_{k+1}$. We also have the ideal $I_\infty = \cup_k I_k = \{n \in \mathbf{Z} \mid \exists p(x) \in I, p(x) = nx^k + a_{k-1}x^{k-1} + \cdots + a_0\}$, i.e. the set of leading terms of elements of I. This is an ideal since the I_k are all ideals and $I_\ell \subseteq I_k$ for all $\ell \leq k$.

Explicitly, let $n, m \in I_\infty$, so there are $p(x), q(x) \in I$ with $p(x) = nx^k + a_{k-1}x^{k-1} + \cdots + a_0, q(x) = mx^\ell + b_{\ell-1}x^{\ell-1} + \cdots + b_0$. Assume without loss of generality that $\ell \leq k$. Then since $p(x), q(x) \in I$, we have for any $d \in \mathbf{Z}$, $(n + dm)x^k + c_{k-1}x^{k-1} + \cdots + c_0 = p(x) + dx^{k-\ell}q(x) \in I$. Thus, $n + dm \in I_\infty$ for any $d \in \mathbf{Z}$, so I_∞ is an ideal.

Since $\mathbf{Z}$ is a PID, $I_\infty = d\mathbf{Z}$ for some $d \in \mathbf{Z}$, i.e. the leading term of every element of I is divisible by d. We have the infinite chain of inclusions of ideals $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq I_\infty = d\mathbf{Z}$. Since $d \in I_\infty = \cup_k I_k$, we have that $d \in I_{k_0}$ for some k_0. Thus, $I_\infty = d\mathbf{Z} \subseteq I_{k_0} \subseteq I_\infty$, so $I_{k_0} = I_\infty$. In other words, the fact that $I_\infty = d\mathbf{Z}$ is finitely generated, which depends only on $\mathbf{Z}$ being noetherian, implies that the chain stabilizes.

Since $d \in I_{k_0}$, let $p_0(x) \in I$ be such that $p_0(x) = dx^{k_0} + a_{k_0-1}x^{k_0-1} + \cdots + a_0$. Now, if $q(x) \in I$ has degree $\ell \geq k$, we have $q(x) = (b_\ell d)x^\ell + b_{\ell-1}x^{\ell-1} + \cdots + b_0$. Thus, $q(x) - b_\ell x^{\ell-k}p_0(x)$ has degree $\ell - 1$. Repeating this process, we see that $q(x) = r(x)p_0(x) + q'(x)$ where $q'(x)$ has degree less than k. Thus, $p_0(x)$ together with the set $\{\alpha(x) \in I \mid \deg \alpha < k\} = I \cap (\mathbf{Z}[x])_{<k}$ generates the ideal I over $\mathbf{Z}[x]$. But the $\mathbf{Z}$-module $(\mathbf{Z}[x])_{<k}$ consisting of all polynomials in $\mathbf{Z}[x]$ of degree less than k is a finite free $\mathbf{Z}$-module, and $I \cap (\mathbf{Z}[x])_{<k}$ is a $\mathbf{Z}$-submodule. This implies that it is finitely generated over $\mathbf{Z}$ (indeed, we even know that it

is necessarily free [6]), so it is certainly finitely generated over $\mathbf{Z}[x]$. Taking a finite $\mathbf{Z}[x]$-generating set for this module along with $p_0(x)$ gives the required finite set of generators of I. $\square$

However, there are ideals which require arbitrarily large generating sets. For each $k > 0$, consider the ideal $I_k = (2^k, 2^{k-1}x, 2^{k-2}x^2, \ldots, x^k)$. We claim that this requires $k+1$ generators, i.e. that any smaller generating set will not suffice.

To see this, first note that $I_k = (2, x)^k$, since the $k+1$ given generators are all possible degree k monomials in 2 and x. $(2, x)$ is a maximal ideal, since $R/(2, x) \simeq \mathbf{Z}/2 = \mathbf{F}_2$, which is a field. Now, consider the module $M_k = I_k/I_{k+1} = I_k/(2, x)I_k$. This is a finitely generated module over the R-algebra $\mathbf{F}_2 = R/(2, x)$. Thus, it is a vector space of finite dimension over $\mathbf{F}_2$. Since I_k is spanned by $2^k, 2^{k-1}x, \ldots, x^k$, M_k is spanned by these elements, so it has $\mathbf{F}_2$-dimension at most $k+1$. We want to show that these elements are actually linearly independent over $\mathbf{F}_2$. This is equivalent to showing that if

$$\epsilon_0 2^k + \epsilon_1 2^{k-1} x + \cdots + \epsilon_k x^k \in I_{k+1} \tag{2}$$

for $\epsilon_i \in \{0, 1\}$ then $\epsilon_i = 0$ for all i. If Equation (2) holds, then we can write:

$$\epsilon_0 2^k + \cdots + \epsilon_k x^k = 2^{k+1} p_0(x) + 2^k x p_1(x) + \cdots + x^{k+1} p_{k+1}(x)$$

with $p_i(x) = a_{0,i} + a_{1,i}x + \cdots + a_{d_i,i}x^{d_i} \in \mathbf{Z}[x]$. By comparing the constant terms on each side, we get that $\epsilon_0 2^k = 2^{k+1} a_{0,0}$, so $\epsilon_0 = 2a_{0,0}$, so since $\epsilon_0 \in \{0, 1\}$, we get $\epsilon_0 = a_{0,0} = 0$. Now, comparing degree-one terms on both sides, we get that $\epsilon_1 2^{k-1} = 2^{k+1} a_{1,0} + 2^k a_{1,1}$, so $\epsilon_1 = 2(2a_{1,0} + a_{1,1})$, and $\epsilon_1 = 0$. Continuing in this manner, we see that $\epsilon_i = 0$ for each i, as desired.

Now, if I_k can be generated over R by m elements $a_1, \ldots, a_m \in \mathbf{Z}[x]$, certainly the quotient module I_k/I_{k+1} can be as well. Thus, we must have $m \geq \dim_{R/(2,x)} I_k/I_{k_1} = k+1$.

Question 5. Let V be a finite-dimensional vector space over R, and let $T\colon V \to V$ be a linear transformation. Let $V_{\mathbf{C}} := V \otimes_{\mathbf{R}} \mathbf{C}$. By functoriality we have a map $T_{\mathbf{C}}\colon V_{\mathbf{C}} \to V_{\mathbf{C}}$, defined by $T_{\mathbf{C}}(v \otimes z) = T(v) \otimes z$, called the *complexification* of T; this is a $\mathbf{C}$-linear transformation.

Without using the structure theorem for PIDs or rational canonical form, prove that the minimal polynomial $m_{T_{\mathbf{C}}} \in \mathbf{C}[t]$ is equal to the minimal polynomial $m_T \in \mathbf{R}[t]$ (just prove it directly!); in particular, $m_{T_{\mathbf{C}}}$ has coefficients in $\mathbf{R}$.

Solution. We will use the following lemma:

Lemma 7. If $p(t) \in \mathbf{R}[t]$ is a polynomial with real coefficients, $p(T_{\mathbf{C}}) = 0$ iff $p(T) = 0$.

Proof. Let $p(t) = a_n t^n + \cdots + a_0 \in \mathbf{R}[t] \subseteq \mathbf{C}[t]$ be a polynomial. Then $p(T_{\mathbf{C}}) = (p(T))_{\mathbf{C}}$:

$$\begin{aligned} p(T_{\mathbf{C}})(v \otimes z) &= a_n (T_{\mathbf{C}})^n (v \otimes z) + \cdots + a_0 (v \otimes z) \\ &= a_n (T^n(v) \otimes z) + \cdots + a_0 (v \otimes z) \\ &= (a_n T^n(v) + a_{n-1} T^{n-1}(v) + \cdots + a_0) \otimes z \\ &= p(T)_{\mathbf{C}} (v \otimes z) \end{aligned}$$

[6] This step works for general noetherian rings, where the detailed structure theory of $\mathbf{Z}$-modules is not available: we just need the fact(/definition) that a submodule of a finitely generated module over a noetherian ring is finitely generated.

Here, we used that $(T_{\mathbf{C}})^n(v\otimes z) = (T_{\mathbf{C}})^{n-1}(T_{\mathbf{C}}(v\otimes z)) = (T_{\mathbf{C}})^{n-1}(T(v)\otimes z) = \cdots = T^n(v)\otimes z$, which follows from the definition of $T_{\mathbf{C}}$ (more generally, $(S\circ T)_{\mathbf{C}} = S_{\mathbf{C}}\circ T_{\mathbf{C}}$), as well as the fact that for $a\in\mathbf{R}$, $a(v\otimes z) = v\otimes az = av\otimes z$, since the tensor product is over $\mathbf{R}$.

Now, clearly if $S=0$, then $S_{\mathbf{C}}=0$. Conversely, if $S_{\mathbf{C}}=0$, then for all $v\in V, z\in\mathbf{C}$, we have $S_{\mathbf{C}}(v\otimes z) = S(v)\otimes z = 0$. In particular, $S(v)\otimes 1 = 0$ for all $v\in V$. But since $\mathbf{R}\to\mathbf{C}$ is injective, and V is a free and therefore flat $\mathbf{R}$-module, the map $V\to V_{\mathbf{C}}$ given by $v\mapsto v\otimes 1$ is injective. (Of course, invoking flatness here is silly since $\mathbf{C} = \mathbf{R}1\oplus\mathbf{R}i$, and we can take real and imaginary parts). Thus, if $S(v)\otimes 1 = 0$ for all $v\in V$, we have $S(v)=0$ for all $v\in V$, so $S=0$. Applying this to $p(T_{\mathbf{C}}) = p(T)_{\mathbf{C}}$, we see that $p(T_{\mathbf{C}})=0$ iff $p(T)=0$, as desired.

Alternatively [TC: this is the more straightforward way to do it], we may write $V_{\mathbf{C}} = V\otimes_{\mathbf{R}}\mathbf{C} = V\otimes_{\mathbf{R}}(\mathbf{R}1\oplus\mathbf{R}i) = (V\otimes 1)\oplus(V\otimes i)$ as an $\mathbf{R}$-module. We may thus write any $w\in V$ as v_1+iv_2 with $v_1,v_2\in V$ (i.e. $w = v_1\otimes 1 + v_2\otimes i$). Then we have

$$\begin{aligned}
p(T_{\mathbf{C}})(w) &= p(T_{\mathbf{C}})(v_1+iv_2)\\
&= p(T_{\mathbf{C}})(v_1) + p(T_{\mathbf{C}})(iv_2)\\
&= p(T)_{\mathbf{C}}(v_1\otimes 1) + p(T)_{\mathbf{C}}(v_2\otimes i)\\
&= p(T)(v_1)\otimes 1 + p(T)(v_2)\otimes i
\end{aligned}$$

Thus, $p(T_{\mathbf{C}})(w)=0$ iff $p(T)(v_1) = p(T)(v_2) = 0$. □

Now, since $p(T)=0$ iff $m_T\mid p(T)$ in $\mathbf{R}[t]$, and $p(T_{\mathbf{C}})=0$ iff $m_{T_{\mathbf{C}}}\mid p(T)$ in $\mathbf{C}[t]$, we see that $m_T\mid p(T)$ in $\mathbf{R}[t]$ iff $m_{T_{\mathbf{C}}}\mid p(T)$ in $\mathbf{C}[t]$. In particular, $m_{T_{\mathbf{C}}}\mid m_T$ in $\mathbf{C}[t]$.

By the lemma, in order to conclude the converse direction that $m_T\mid m_{T_{\mathbf{C}}}\in\mathbf{C}[t]$, and thus $m_T = m_{T_{\mathbf{C}}}$ (since both are required by definition to be monic), we need to show that $m_{T_{\mathbf{C}}}\in\mathbf{R}[t]$. Equivalently, $m_{T_{\mathbf{C}}} = \overline{m_{T_{\mathbf{C}}}}$, where $\overline{p(t)}$ denotes complex conjugation in $\mathbf{C}[t]$ (i.e. $\overline{a_0+a_1t+\cdots+a_nt^n} = \overline{a_0}+\overline{a_1}t+\cdots+\overline{a_n}t^n$). Now, we will conclude by the following lemma:

Lemma 8. If $T\colon V\to V$ is a linear transformation, then if $p(t)\in\mathbf{C}[t]$ is a polynomial, $p(T_{\mathbf{C}})(v\otimes z) = \overline{\overline{p}(T_{\mathbf{C}})(v\otimes\overline{z})}$ for any $v\in V$, $z\in\mathbf{C}$. Here, complex conjugation is defined on $V_{\mathbf{C}}$ by $\overline{v\otimes z} = v\otimes\overline{z}$

This lemma suffices for the proof, since in particular it implies that $p(T_{\mathbf{C}})=0$ iff $\overline{p}(T_{\mathbf{C}})=0$. Thus, $\overline{m_{T_{\mathbf{C}}}}(T_{\mathbf{C}})=0$, so $m_{T_{\mathbf{C}}}\mid\overline{m_{T_{\mathbf{C}}}}$, and since these are monic polynomials of the same degree, we conclude that $m_{T_{\mathbf{C}}} = \overline{m_{T_{\mathbf{C}}}}$, as desired. Now, we are left to prove the lemma:

Lemma 9. Let $p(t) = z_0+z_1t+\cdots+z_nt^n$ with $z_i\in\mathbf{C}$. Let $z_i = a_i+ib_i$ with $a_i,b_i\in\mathbf{R}$. Now, we may compute:

$$\begin{aligned}
\overline{\overline{p}(T_{\mathbf{C}})(v\otimes\overline{z})} &= \overline{\overline{z_0}(v\otimes\overline{z}) + \overline{z_1}T_{\mathbf{C}}(v\otimes\overline{z}) + \cdots + \overline{z_n}(T_{\mathbf{C}})^n(v\otimes\overline{z})}\\
&= \overline{\overline{z_0}(v\otimes\overline{z}) + \overline{z_1}(T(v)\otimes\overline{z}) + \cdots + \overline{z_n}(T^n(v)\otimes\overline{z})}\\
&= \overline{v\otimes\overline{z_0z} + T(v)\otimes\overline{z_1z} + \cdots + T^n(v)\otimes\overline{z_nz}}\\
&= v\otimes z_0z + T(v)\otimes z_1z + \cdots + T^n(v)\otimes z_nz\\
&= (z_0 + T_{\mathbf{C}} + \cdots + T_{\mathbf{C}}^n(v))(v\otimes z)\\
&= p(T_{\mathbf{C}})(v\otimes z)
\end{aligned}$$

Let V and W be finite-dimensional vector spaces over $\mathbf{R}$, and let $\omega_V : V \times V \to \mathbf{R}$ and $\omega_W : W \times W \to \mathbf{R}$ be positive definite symmetric forms. Given a linear transformation $T\colon V \to W$, the *adjoint* $T^*\colon W \to V$ is defined as follows (first verbosely, but see (ADJ) below for a self-contained definition).

Recall that the nondegeneracy of ω_V means that ω induces an isomorphism $V \to V^\vee$. Concretely, this means that for every linear map $\lambda\colon V \to \mathbf{R}$ there is a unique vector v such that $\omega_V(v, x) = \lambda(x)$. For a given $w \in W$, the function $\lambda_w\colon V \to \mathbf{R}$ given by $\lambda_w\colon v \mapsto \omega_W(T(v), w)$ is a linear map from V to $\mathbf{R}$. We define $T^*(w) \in V$ to be the vector corresponding as above to λ_w. In other words, T^* is defined by the identity

$$\omega_W(T(v), w) = \omega_V(v, T^*(w)) \quad \text{for all } v \in V \text{ and all } w \in W \tag{ADJ}$$

It is very straightforward to verify from this definition the following properties:
(i) T^* is an $\mathbf{R}$-linear transformation;
(ii) $(T_1 + T_2)^* = T_1^* + T_2^*$ and $(cT)^* = c(T^*)$ for $c \in \mathbf{R}$;
(iii) $(S \circ T)^* = T^* \circ S^*$.

Question 6. Let V be a finite-dimensional vector space over $\mathbf{R}$, and let $\omega_V\colon V \times V \to \mathbf{R}$ be a positive definite symmetric form. An endomorphism $T\colon V \to V$ is called *self-adjoint* if $T^* = T$.

Suppose that $T\colon V \to V$ is self-adjoint. Prove that the minimal polynomial $m_T \in \mathbf{R}[t]$ splits completely (i.e. $m_T(t) = (t - \lambda_1)(t - \lambda_2)\cdots(t - \lambda_n)$ for some $\lambda_1, \ldots, \lambda_n \in \mathbf{R}$). (For the different linear maps or bilinear forms you use in the proof, be *very* careful to make clear what the domain and codomain are, and to what extent they are linear/bilinear; this is the key point of the problem.)

Solution. Any monic polynomial $p(t) \in \mathbf{R}[t]$ of degree n factors in $\mathbf{C}[t]$ as

$$p(t) = [(t - \lambda_1)(t - \overline{\lambda_1})][(t - \lambda_2)(t - \overline{\lambda_2})]\cdots[(t - \lambda_k)(t - \overline{\lambda_k})](t - \tau_1)\cdots(t - \tau_{n-2k})$$

with $\tau_i \in \mathbf{R}$, $\lambda_i \in \mathbf{C} - \mathbf{R}$. Thus, to show that m_T splits completely in $\mathbf{R}$, it is necessary and sufficient to show that all of the roots of m_T over $\mathbf{C}$ are real. By Question 6, $m_T = m_{T_\mathbf{C}}$, so it is equivalent to show that all of the roots in $\mathbf{C}$ of $m_{T_\mathbf{C}}$ are real. But these are exactly the eigenvalues of $T_\mathbf{C}$, so we need to show that the eigenvalues of $T_\mathbf{C}$ are real.

In order to do this, we need to extend ω_V to a form on $V_\mathbf{C}$, so we can make sense of the property of being self-adjoint. The notion of positive-definite symmetric form does not make sense over $\mathbf{C}$: if ω is a $\mathbf{C}$-bilinear form on $V_\mathbf{C}$, then $\omega(iv, iv) = i^2\omega(v, v) = -\omega(v, v)$, so positive-definiteness is lost.

A replacement for complex vector spaces is the notion of a *hermitian form*. If W is a complex vector space, a $\mathbf{C}$-semilinear form $\omega(\cdot, \cdot)$ on W is an $\mathbf{R}$-bilinear form such that $\omega(zw_1, w_2) = z\omega(w_1, w_2)$, and $\omega(w_1, w_2) = \overline{\omega(w_2, w_1)}$ for all $z \in \mathbf{C}, w_i \in W$. Note that in particular, this implies that we have $\omega(w_1, zw_2) = \overline{\omega(zw_2, w_1)} = \overline{z}\overline{\omega(w_2, w_1)} = \overline{z}\omega(w_1, w_2)$, and $\omega(w, w) = \overline{\omega(w, w)}$, so $\omega(w, w) \in \mathbf{R}$ for all $w \in W$. A *hermitian form* on W is a $\mathbf{C}$-semilinear form such that $\omega(w, w) > 0$ for all $w \in W - \{0\}$. The notion of adjoints still make sense with respect to hermitian forms: as above, if T is a $\mathbf{C}$-linear transformation acting on W, we define T^* by:

$$\omega(T(v), w) = \omega(v, T^*(w))$$

for all $v, w \in W$. Just as in the real case, we can show that this makes sense via non-degeneracy. ω is non-degenerate in the sense that if $\omega(w, v) = 0$ for all $w \in W$, then $v = 0$, since we may take $w = v$ and $\omega(v, v) > 0$ unless $v = 0$. Likewise, if $\omega(v, w) = 0$ for all $w \in W$, then $v = 0$. Thus, the map $\widetilde{\omega}\colon W \to W^\vee$ which sends w to $\widetilde{\omega}(w)\colon v \mapsto \omega(v, w)$ is injective. Note that since $\omega(zv, w) = z\omega(v, w)$ for $z \in \mathbf{C}$, this map really does produce a $\mathbf{C}$-linear form on W. However, the map $\widetilde{\omega}$ itself is not $\mathbf{C}$-linear, since $\widetilde{\omega}(zw) = \overline{z}\widetilde{\omega}(w)$. Nonetheless, it is an injective $\mathbf{R}$-linear map between real vector spaces of the same dimension, and thus it is a isomorphism of real vector spaces which is moreover "conjugate-linear" in $\mathbf{C}$. We then may define $T^*(w)$ for $w \in W$ to be the unique element of W such that $\widetilde{\omega}(T^*(w)) = \widetilde{\omega}(w) \circ T$. Unwinding the definitions, this says exactly that for all $v \in W$, $\omega(v, T^*(w)) = \omega(T(v), w)$.

Note that the definition above forces T^* to be $\mathbf{C}$-linear (it is clearly $\mathbf{R}$-linear, since $T^* = \widetilde{\omega}^{-1} \circ T^\vee \circ \widetilde{\omega}$ is a composite of $\mathbf{R}$-linear maps): we have $\omega(v, T^*(zw)) = \omega(T(v), zw) = \overline{z}\omega(T(v), w) = \overline{z}\omega(v, T^*(w)) = \omega(v, zT^*(w))$ for all $z \in \mathbf{C}$, $v, w \in W$. Then, by non-degeneracy, this implies that $T^*(zw) = zT^*(w)$ for all $z \in \mathbf{C}, w \in W$. In other words, the conjugate-linearity of $\widetilde{\omega}$ and $\widetilde{\omega}^{-1}$ "cancel out" to get a $\mathbf{C}$-linear map.

Now, we want to extend ω_V to a hermitian form $\omega_{\mathbf{C}}$ on $V_{\mathbf{C}}$ in such a way that $(T^*)_{\mathbf{C}} = (T_{\mathbf{C}})^*$.

The obvious choice of $\omega_{\mathbf{C}}$ is:

$$\omega_{\mathbf{C}}(v \otimes z, v' \otimes z') = z\overline{z'} \cdot \omega(v, v')$$

In other words, we have:

$$\omega_{\mathbf{C}}(v_1 + iv_2, w_1 + iw_2) = \omega(v_1, w_1) + \omega(v_2, w_2) + i\left(\omega(v_2, w_1) - \omega(v_1, w_2)\right) \tag{3}$$

We need to check that this is hermitian. It is clearly $\mathbf{R}$-bilinear. To check the identities $\omega_{\mathbf{C}}(zw_1, w_2) = z\omega_{\mathbf{C}}(w_1, w_2)$ and $\omega_{\mathbf{C}}(w_2, w_1) = \overline{\omega_{\mathbf{C}}(w_1, w_2)}$, by $\mathbf{R}$-bilinearity it suffices to consider the case that $w_i = v_i \otimes z_i$. Then, we have

$$\omega_{\mathbf{C}}(z(v_1 \otimes z_1), v_2 \otimes z_2) = zz_1\overline{z_2}\omega(v_1, v_2) = z\omega_{\mathbf{C}}(w_1, w_2)$$

and

$$\omega_{\mathbf{C}}(v_2 \otimes z_2, v_1 \otimes z_1) = z_2\overline{z_1}\omega(v_2, v_1) = z_2\overline{z_1}\omega(v_1, v_2) = \overline{z_1\overline{z_2}\omega(v_1, v_2)} = \overline{\omega(w_1, w_2)}$$

Here, we used that ω is symmetric and that $\omega(v_1, v_2) \in \mathbf{R}$ for any $v_1, v_2 \in V$. Thus, $\omega_{\mathbf{C}}$ is $\mathbf{C}$-semilinear. To check that it is hermitian, we need $\omega_{\mathbf{C}}(w, w) > 0$ for $w \in W$. Writing $w = v_1 + iv_2$ (shorthand for $v_1 \otimes 1 + v_2 \otimes i$), we compute by Equation (3):

$$\begin{aligned}\omega_{\mathbf{C}}(v_1 + iv_2, v_1 + iv_2) &= \omega(v_1, v_1) + \omega(v_2, v_2) + i(\omega(v_2, v_1) - \omega(v_1, v_2)) \\ &= \omega(v_1, v_1) + \omega(v_2, v_2) > 0\end{aligned}$$

Here, we used the symmetry and positive-definiteness of ω.

Now, we want to show that $(T^*)_{\mathbf{C}} = (T_{\mathbf{C}})^*$. Recall that $(T_{\mathbf{C}})^*$ is defined by the condition that

$$\omega_{\mathbf{C}}(T_{\mathbf{C}}(w_1), w_2) = \omega_{\mathbf{C}}(w_1, (T_{\mathbf{C}})^*(w_2))$$

for all $w_1, w_2 \in V_{\mathbf{C}}$. By $\mathbf{R}$-bilinearity of $\omega_{\mathbf{C}}$ and $\mathbf{R}$-linearity of $T_{\mathbf{C}}$, it suffices to check this when $w_1 = v_1 \otimes z_1$ and $w_2 = v_2 \otimes z_2$. Thus, in order to prove that $(T_{\mathbf{C}})^* = (T^*)_{\mathbf{C}}$, it suffices to prove that:

$$\omega_{\mathbf{C}}(T_{\mathbf{C}}(w_1 \otimes z_1), w_2 \otimes z_2) = \omega_{\mathbf{C}}(w_1 \otimes z_1, (T^*)_{\mathbf{C}}(w_2 \otimes z_2))$$

Now, we compute:

$$\begin{aligned}\omega_{\mathbf{C}}(T_{\mathbf{C}}(w_1 \otimes z_1), w_2 \otimes z_2) &= \omega_{\mathbf{C}}(T(w_1) \otimes z_1, w_2 \otimes z_2) \\ &= z_1\overline{z_2}\omega(T(w_1), w_2) \\ &= z_1\overline{z_2}\omega(w_1, T^*(w_2)) \\ &= \omega_{\mathbf{C}}(w_1 \otimes z_1, T^*(w_2) \otimes z_2) \\ &= \omega_{\mathbf{C}}(w_1 \otimes z_1, (T^*)_{\mathbf{C}}(w_2 \otimes z_2))\end{aligned}$$

Now, since T is self-adjoint, we have $T_{\mathbf{C}} = (T^*)_{\mathbf{C}} = (T_{\mathbf{C}})^*$, so $T_{\mathbf{C}}$ is self-adjoint with respect to the hermitian form $\omega_{\mathbf{C}}$. We want to show that its eigenvalues are real, so assume that $w \in V_{\mathbf{C}}, w \neq 0$ is such that $T_{\mathbf{C}}(w) = \lambda w$ for $\lambda \in \mathbf{C}$. For any $v \in V$, we compute:

$$\begin{aligned}
\lambda\omega_{\mathbf{C}}(w, w) &= \omega_{\mathbf{C}}(\lambda w, w) \\
&= \omega_{\mathbf{C}}(T_{\mathbf{C}}(w), w) \\
&= \omega_{\mathbf{C}}(w, T_{\mathbf{C}}(w)) \\
&= \omega_{\mathbf{C}}(w, \lambda w) \\
&= \overline{\lambda}\omega_{\mathbf{C}}(w, w)
\end{aligned}$$

Thus, since $\omega_{\mathbf{C}}(w, w) \neq 0$, we have $\lambda = \overline{\lambda}$, so $\lambda \in \mathbf{R}$ as desired.

We can actually prove even more [though this was not necessary for the HW]: the minimal polynomial m_T splits into *distinct* factors, i.e. T is semi-simple. Since m_T splits over $\mathbf{R}$, every eigenvalue of $T_{\mathbf{C}}$ is already an eigenvalue of T. In particular, T has an eigenvector $v \in V$ with eigenvalue $\lambda \in \mathbf{R}$. Let V_λ be the eigenspace for λ, and let W_λ be the ω-orthogonal complement of V_λ. We claim that W_λ is T-stable: if $w \in W_\lambda$, we have for any $v \in V_\lambda$, $0 = \lambda\omega(v, w) = \omega(\lambda v, w) = \omega(T(v), w) = \omega(v, T(w))$. Thus, $T(w)$ is orthogonal to V_λ. But $T|_{W_\lambda}$ is still self-adjoint with respect to $\omega|_{W_\lambda}$, since the identity $\omega(T(w), w') = \omega(w, T(w'))$ holds for any $w, w' \in \lambda$. Similarly, $\omega|_{W_\lambda}$ is still symmetric and positive-definite. Thus, by induction on $\dim V$, $T|_{W_\lambda}$ is semisimple. Since the direct sum of semisimple transformations is semisimple by HW6, this implies that T is semisimple.