2014 Algebra SEP $\sim$ Grab Bag solutions, by E. Dummit

1. (Jan-97.4) Let K be a field.

   (a) If $\text{char}(K) \neq 2$, show that $GL_n(K)$ has exactly n conjugacy classes of elements of order 2.

   (b) If $\text{char}(K) = 2$, show that $GL_n(K)$ has exactly $\lfloor n/2 \rfloor$ conjugacy classes of elements of order 2.

   Solution: If $A \in GL_n(K)$ has order 2, then the minimal polynomial of A must divide $x^2 - 1$ and cannot equal $x - 1$. In particular, we see that all eigenvalues of A are equal to 1 or to -1. Therefore the Jordan form of A has all entries in K, so A is conjugate over K to its Jordan form (by the usual results on the rational canonical form). Thus it suffices to examine the possible Jordan forms J of A, since these are unique conjugacy-class representatives.

   a) The minimal polynomial of J divides $x^2 - 1$ so all eigenvalues are 1 or -1, and not all can be equal to 1. Furthermore, since $x^2 - 1$ is squarefree, we see that all Jordan blocks are size 1 so J is diagonal, and on its diagonal we must have k copies of -1 and $n - k$ copies of 1, for some $1 \leq k \leq n$. Each such k works, so there are n conjugacy classes.

   b) The minimal polynomial of J divides $x^2 - 1 = (x - 1)^2$ so all eigenvalues are 1, and all Jordan blocks are or size 1 or 2 and they cannot all be of size 1. So we must have k 2×2 blocks and $n - 2k$ 1×1 blocks, for some $1 \leq k \leq \lfloor n/2 \rfloor$; each such k works, so there are $\lfloor n/2 \rfloor$ conjugacy classes.

---

2. (Aug-08.5): Let R be a subring of $M_n(\mathbb{C})$ and suppose R is finitely generated as a $\mathbb{Z}$-module. Let $M \in R$.

   (a) Show that M is contained in a commutative subring S of $M_n(\mathbb{C})$ that is finitely generated as a $\mathbb{Z}$-module.

   (b) Deduce that there is a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(M) = 0$.

   (c) Prove that $\text{tr}(M)$ is an algebraic integer.

   Solution:

   a) The subring of R generated by M is still a finitely-generated $\mathbb{Z}$-module (because $\mathbb{Z}$ is Noetherian), but is also commutative.

   b) The point here is to see that M is integral over $\mathbb{Z}$ (where we embed $\mathbb{Z}$ in S as the diagonal matrices), which by the construction of S is equivalent to S being integral over $\mathbb{Z}$. But this follows immediately because S is finitely generated over $\mathbb{Z}$ and commutative.

   c) In fact all of the eigenvalues of M are algebraic integers, hence (in particular) so is their sum. This follows from part (b): the minimal polynomial for M (which could have nonintegral coefficients) must divide the polynomial $f(x)$. But every eigenvalue is a root of the minimal polynomial hence of $f(x)$, so they are all algebraic integers because they are roots of a monic polynomial with integer coefficients.

---

3. (Aug-94.5) Let F be a field and $S = M_n(F)$.

   (a) If $s \in S$ is nilpotent, show that $\text{tr}(S) = 0$.

   (b) If R is a ring (not necessarily commutative) and $\theta : R \to S$ is a surjective ring homomorphism, let I be an ideal of R such that every element of I is a sum of nilpotent elements of R. Show that $\theta(I) = 0$.

   Solution:

   a) A matrix is nilpotent if and only if all its eigenvalues are zero. The trace is then equal to n times 0.

   b) The point is to use the fact that S is a simple ring: then $\theta(I) = 0$ or $\theta(I) = S$, since θ is surjective (so $\theta(I)$ is an ideal of S). Now if $x \in I$ then by (a) and the fact that trace is additive, we see $\text{tr}(\theta(x)) = 0$, hence $\theta(I)$ cannot be S since $\theta(I)$ contains only trace-zero matrices.

---

4. (Aug-99.5) Let F be a field, $f(x)$ and $g(y)$ be nonconstant polynomials in $R = F[x, y]$, and $I = (f(x), g(y))$, the ideal generated by f and g.

   (a) Show that $I \neq R$.

   (b) If $f(x) = x - \alpha$ and $g(y) = y - \beta$ for $\alpha, \beta \in F$, show that I is a maximal ideal.

Solution:

a) Let α be a root of $f(x)$ in an algebraic closure $\bar{F}$ and β be a root of $g(y)$ in $\bar{F}$. The evaluation map $f_{\alpha,\beta} : R \to \bar{F}$ sending $p(x, y) \mapsto p(\alpha, \beta)$ is nontrivial on R since $f(1) = 1$, but the kernel contains I.

b) The quotient R/I is clearly isomorphic to F (via $\overline{p(x, y)} \mapsto p(\alpha, \beta)$), and F is a field.

Remark Both parts are examples of the Nullstellensatz.

---

5. (Jan-92.5) Let $\alpha_1, \cdots, \alpha_n$ be the roots of the polynomial $f(x) = 2x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$.

   (a) Show that $2\alpha_i$ is an algebraic integer for $1 \leq i \leq n$.

   (b) Show that $\mathbb{Z}[\alpha_1, \cdots, \alpha_n] \cap \mathbb{Q} \subseteq \mathbb{Z}[1/2]$.

   (c) If some a_j with $0 \leq j \leq n - 1$ is odd, show that $1/2 \in \mathbb{Z}[\alpha_1, \cdots, \alpha_n] \cap \mathbb{Q}$, and deduce that the latter intersection is $\mathbb{Z}[1/2]$. What happens if all a_j are even?

Solution:

a) Clearly $2\alpha_i$ is a root of $2^{n-1}f(x/2) = x^n + 2a_{n-1}x^{n-1} + \cdots + 2^{n-1}a_0$, which is monic.

b) Suppose $f(\alpha_1, \cdots, \alpha_n) \in \mathbb{Q}$ where $f \in \mathbb{Z}[x_1, \cdots, x_n]$ has total degree d. Then $2^d f(a_1, \cdots, \alpha_n)$ is a polynomial in $2\alpha_1, \cdots, 2\alpha_n$ (by absorbing a factor of 2 into each appearance of an α, and putting any leftover factors of 2 into the coefficients), hence by (a) it is an algebraic integer and in $\mathbb{Q}$, hence is an integer. Thus we see $f(\alpha_1, \cdots, \alpha_n) \subseteq \mathbb{Z}[1/2]$ as desired.

c) Each coefficient of $\frac{1}{2}f(x) = x^n + \frac{a_{n-1}}{2}x^{n-1} + \cdots$ is a symmetric function in $\alpha_1, \cdots, \alpha_n$, so $\frac{a_{n-1}}{2}, \frac{a_{n-2}}{2}, \cdots$ all lie in $\mathbb{Z}[\alpha_1, \cdots, \alpha_n] \cap \mathbb{Q}$. Ergo if any a_i is odd we get that $1/2 \in \mathbb{Z}[\alpha_1, \cdots, \alpha_n] \cap \mathbb{Q}$ hence $\mathbb{Z}[\alpha_1, \cdots, \alpha_n] \cap \mathbb{Q}$ contains $\mathbb{Z}[1/2]$, so by part (b) we see that the intersection is $\mathbb{Z}[1/2]$. If all a_j are even, then we can obviously divide all coefficients of f by 2 to see that the α_i are algebraic integers, so that $\mathbb{Z}[\alpha_1, \cdots, \alpha_n] \cap \mathbb{Q} = \mathbb{Z}$.

---

6. (Jan-12.5): Let K be a field where -1 is not a square, and let $G = GL_2(K)$.

   (a) If $g \in G$, show that g has order 4 iff $\det(g) = 1$ and $\operatorname{tr}(g) = 0$.

   (b) Find explicitly an element $g \in G$ of order 4.

   (c) Suppose there exist elements $a, b \in K$ with $a^2 + b^2 = -1$. Show that G contains two elements g, h of order 4 such that gh also has order 4.

Solution:

a) Since -1 is not a square in K, $x^2 + 1$ is irreducible over K. Now, g has order 4 iff $g^4 = 1$ and $g^2 \neq 1$, iff $(g^2 - 1)(g^2 + 1) = 0$ and $g^2 - 1 \neq 0$, iff the minimal polynomial of g divides $(x^2 - 1)(x^2 + 1)$ but not $x^2 - 1$. Since g is a 2×2 matrix, this last statement is equivalent to the minimal polynomial (and characteristic polynomial) of g being $x^2 + 1$. Finally, $x^2 - \operatorname{tr}(g)\, x + \det(g) = \operatorname{charpoly}(x) = x^2 + 1$ is equivalent to $\det(g) = 1$ and $\operatorname{tr}(g) = 0$.

b) All such matrices are conjugate over K; thus: $A^{-1}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}A$ for any $A \in G$.

c) In fact such g and h exist if and only if there exist $a, b \in K$ with $a^2 + b^2 = -1$: by conjugating we can assume $g = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Then we need $h = \begin{pmatrix} p & q \\ r & -p \end{pmatrix}$ to be such that $-p^2 - qr = 1$ and such that $gh = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} r & -p \\ -p & -q \end{pmatrix}$ has trace 0 (its determinant is automatically 1): thus we require $q = r$, and the only remaining condition is $p^2 + r^2 = -1$.

---

7. (Jan-96.5) Let q be a prime power and $f(x) = \dfrac{x^5-1}{x-1} = x^4+x^3+x^2+x+1 \in \mathbb{F}_q[x]$.

   (a) If f has a root in $\mathbb{F}_q$, show that f splits completely over $\mathbb{F}_q$ and show that this happens precisely when $q \equiv 0, 1 \bmod 5$.

   (b) If $f(x)$ has an irreducible monic factor $g(x)$ of degree 2, show that g has constant term 1.

   (c) Factor $f(x)$ into quadratic factors when $q = 29$.

Solution:

a) We see that the roots of $f(x)$ are fifth roots of unity in $\overline{\mathbb{F}_q}$. If 5 divides q then $f(x) = (x-1)^4$ clearly splits completely. Now assume 5 does not divide q: then x^5-1 and its derivative are relatively prime hence f is separable, and if ζ is any root of f then the other roots of f are $\zeta^2, \zeta^3, \zeta^4$ (which are distinct by separability) so f has a root iff it splits completely. Finally, f has a root iff $\mathbb{F}_q^\times$ has an element of order 5, which happens precisely when $\left|\mathbb{F}_q^\times\right| = q-1$ is divisible by 5.

b) If f has an irreducible quadratic factor then by (a) it must factor as a product of two irreducible quadratics, and the four roots of f are $\zeta, \zeta^2, \zeta^3, \zeta^4$, none of which are in $\mathbb{F}_q$. The constant term of g is then the product of two of the four roots, and so the only possibility is that this product is 1, since it must be a power of ζ and the only power of ζ in $\mathbb{F}_q$ is 1.

c) By (b) and comparing coefficients, we see that f must factor as $(x^2+ax+1)(x^2+(1-a)x+1)$, where $a(1-a)+2 = 1$, hence $a^2-a-1 = 0$, hence $a = \dfrac{1 \pm \sqrt{5}}{2} = \dfrac{1 \pm 11}{2} = \{6, -5\}$ in $\mathbb{F}_{29}$. Thus the desired factorization is $(x^2+6x+1)(x^2-5x+1)$.

Remark In fact we can completely characterize how f splits depending on q: it suffices to analyze the degree of the field extension $\mathbb{F}_q[\zeta_5]/\mathbb{F}_q$. Since all finite fields are splitting fields, as soon as we adjoin one root, we get all the others (so all the irreducible factors of f must be the same degree), so we need only determine the smallest power q^d such that $\mathbb{F}_{q^d}$ contains an element of multiplicative order 5. But this is the smallest d for which 5 divides $\left|\mathbb{F}_{q^d}^\times\right| = q^d - 1$, which is simply the order of q in $(\mathbb{Z}/5\mathbb{Z})^\times$. So if q is zero or has order 1 ($q \equiv 0, 1 \bmod 5$), the polynomial splits completely, if it has order 2 ($q \equiv 4 \bmod 5$) it factors into two irreducible quadratics, and if it has order 4 ($q \equiv 2, 3 \bmod 5$) it is irreducible.

---

8. (Jan-01.5) Let V be a finite-dimensional F-vector space and $T : V \to V$. Assume that no nonzero proper subspace of V is mapped into itself by T.

   (a) If $S \in F[T]$ is nonzero, show that $\{v \in V : Sv = 0\}$ is the zero subspace.

   (b) Prove that $F[T]$ is a field.

   (c) Show that $|F[T] : F| = \dim_F V$.

Solution: In the usual way, we observe that $F[T]$ is an $F[x]$-module, where x acts as T. Since $F[x]$ is a PID, we can apply the structure theorem for modules over PIDs to see $F[T] \cong \bigoplus F[x]/(p_i(x))$ for some polynomials p_i.

a) Let $W = \{v \in V : Sv = 0\}$ and pick any $w \in W$. Since S is a polynomial in T, $STw = TSw = 0$, hence $Tw \in W$. Thus W is mapped into itself by T, so $W = 0$.

b) There cannot be more than one term in the direct sum as otherwise we could take $S = p_2(T)$ and derive a contradiction to part (a). Furthermore, $p_1(x)$ must be irreducible, or we could break apart the direct sum further by the Chinese Remainder Theorem, so $F[T] \cong F[x]/(p_1(x))$ is a field.

c) From the structure theorem, we know that the product of all the polynomials $p_i(x)$ is the characteristic polynomial of T, which has degree $\dim_F V$. But there is only one polynomial $p_1(x)$, so $\deg(p_1) = \dim_F V$. Since $F[T] \cong F[x]/(p_1(x))$, we are done.

Note In fact, the argument in part (b) proves the more general fact that there are no nonzero proper T-invariant subspaces if and only if the characteristic and minimal polynomials of T are equal.

---

9. (Jan-11.2) Let R be a commutative ring with 1, $(a) = aR$, and P a prime ideal properly contained in (a).

   (a) Show that $P = aP$.

   (b) If P is finitely generated, prove there exists $b \in R$ with $(1 - ab)P = 0$.

   (c) If R is a domain, conclude that either $P = 0$ or $(a) = R$.

Solution:

a) Clearly $aP \subseteq P$. Now let $x \in P$: since $x \in (a)$, we have $x = az$ for some $z \in R$. As P is prime and $a \notin P$ (by proper containment), we have $z \in P$. Hence $x = az$ for some $z \in P$, so we conclude $P \subseteq aP$, so they are equal.

b) Suppose that P is generated by $x_1, \cdots, x_n$ as an R-module. By part (a) applied in turn to $x_1, \cdots, x_n$, there exists a matrix A such that $\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = A \cdot a \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$; then $(I - aA) \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$. By linear algebra, we can therefore take $1 - ab = \det(I - aA)$. [Note that this makes sense because every term in the determinant expansion will have an a, except for the one on the main diagonal]

Remark The fact that $B \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ implies $\det(B)\, x_i = 0$ for every x_i follows immediately by left-multiplying by the cofactor matrix of B.

c) If $P = 0$ we are done. Otherwise, if $x \in P$ is nonzero, we get $(1 - ab)x = 0$ whence $1 - ab = 0$ whence a is a unit whence $(a) = R$.

---

10. (Jan-07.5) Let A be an additive abelian group and B a subgroup. We say B is essential in A (B ess A) if $B \cap X \neq 0$ for every nontrivial subgroup of A.

   (a) If B_1 ess A_1 and B_2 ess A_2 show that $(B_1 \oplus B_2)$ ess $(A_1 \oplus A_2)$.

   (b) If B ess A and B has no nonzero elements of finite order, show A has no nonzero elements of finite order.

   (c) If $\mathbb{Q}$ ess A for some abelian group A, show that $A = \mathbb{Q}$.

Solution:

a) Let X be a nontrivial subgroup of $A = A_1 \oplus A_2$ and π_1, π_2 be the projection maps into A_1 and A_2 respectively. If X contains an element of the form $(x, 0)$ with $x \neq 0$ then since B_1 is essential in A_1 we see that $\langle (x, 0) \rangle \cap B_1 \neq 0$ so $X \cap B \neq 0$ and we are done. Now let $(x, y) \in A$ with $x, y \neq 0$: since B_1 is essential in A_1 there exists n such that $nx \in B$ and $nx \neq 0$. If $ny = 0$ then $n(x, y) = (nx, 0)$ is of the form $(*, 0)$ and we are done. Otherwise, if $ny \neq 0$, there exists an m such that $mny \in B_2$ and $mny \neq 0$: then $mn(x, y) \in X \cap (B_1 \oplus B_2)$ and is not zero.

b) If $g \in A$ has finite order, then since B is essential, $B \cap \langle g \rangle \neq 0$, but every nontrivial element of $\langle g \rangle$ has finite order, hence $\langle g \rangle = 0$ so $g = 0$.

c) By part (b) we see that A has no nonzero elements of finite order. Now suppose $x \in A$: by hypothesis $\mathbb{Q} \cap \langle x \rangle \neq 0$ so say $kx = \frac{p}{q} \in \mathbb{Q}$; then $k(x - \frac{p}{kq}) = 0$ hence since the only element of finite order is 0, we see $x - \frac{p}{kq} = 0$ so $x = \frac{p}{kq} \in \mathbb{Q}$.

---

11. (Jan-08.4) Let V be a finite-dimensional vector space over F of characteristic p, $T : V \to V$, and $W = \{v \in V : Tv = v\}$. Further suppose $T^p = I$ and $\dim_F W = 1$.

(a) Show that $(T - I)^p = 0$ and that $\dim_F V \leq p$.

(b) If $\dim_F V < p$ show that $(T - I)^{p-1} = 0$.

(c) If there exists $v \in V$ with $v + Tv + T^2 v + \cdots + T^{p-1} v \neq 0$, show $\dim_F V = p$.

Solution:

a) Since we are in characteristic p we have $0 = T^p - I = (T - I)^p$, so V is equal to the generalized 1-eigenspace of T. Now if we choose any basis for V and let A be the matrix for T, then over $\bar{F}$ the Jordan form of A has all Jordan blocks of eigenvalue 1 – hence the Jordan form of A has only entries 0 and 1 hence is in F, so (by the standard result that two matrices in $M_n(F)$ are conjugate over $\bar{F}$ iff they are conjugate over F) we can assume A is in Jordan form. Now A cannot have more than 1 Jordan block since $\dim_F W = 1$, and each Jordan block carries an eigenvector, and since $(T - I)^p = 0$ this Jordan block must have size at most p.

b) By part (a) we see the characteristic polynomial of T is $(T - I)^{\dim(V)}$, so if $\dim(V) < p$ we see $(T - I)^{p-1} = 0$.

c) We have $(x - I)^{p-1} = \dfrac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1$. Now applying this to T shows that $v \notin \ker (T - I)^{p-1}$ so $(T - I)^{p-1} \neq 0$ so by the contrapositive of (b) we see $\dim_F V \geq p$ hence we get equality by (a).

---

12. (Aug-11.2) Let R be a commutative ring with 1 and Q a primary ideal of R. For any $a \in R \backslash Q$, define the ideal $I_a = \{r \in R : ar \in Q\}$.

(a) Show that $\mathrm{rad}(I_a) = \mathrm{rad}(Q)$.

(b) Show that I_a is a primary ideal of R.

(c) If R is Noetherian, show that there exists an a such that that I_a is a prime ideal.

Solution:

a) First observe that I_a contains Q, so $\mathrm{rad}(I_a) \supseteq \mathrm{rad}(Q)$. Now suppose that $x \in \mathrm{rad}(I_a)$ so that $x^n \in I_a$: then $ax^n \in Q$, so since Q is primary, $a \in Q$ or $x^{mn} \in Q$ for some m. Since $a \notin Q$, we see $x^{mn} \in Q$, so $x \in \mathrm{rad}(Q)$.

b) Suppose that $xy \in I_a$, so that $axy \in Q$. Since Q is primary, we have $ax \in Q$ or $y^n \in Q \iff ax \in Q$ or $ay^n \in Q \implies x \in I_a$ or $y^n \in I_a$, as desired.

c) Construct an ascending chain of ideals in the following way: choose any $a_1 \notin Q$ and consider I_{a_1}. If this ideal is not prime, say $xy \in I_{a_1}$ with $x, y \notin I_{a_1}$ – then $a_1 x$, $a_1 y \notin I_{a_1}$ – and let $a_2 = a_1 x$. Then I_{a_2} strictly contains I_{a_1} (since if $a_1 r \in Q$ then $a_1 x r \in Q$, and I_{a_2} contains x while I_{a_1} does not). Continue this procedure: since R is Noetherian it must eventually terminate, and at that point the last ideal I_{a_k} is prime.

---

13. (Aug-07.2) Let R be a commutative integral domain that is integrally closed in its field of fractions F.

(a) Suppose K is a field containing F and $\alpha \in K$ is integral over R. Show that the minimal monic polynomial of α over F is in $R[x]$.

(b) Let $f(x) \in R[x]$ be monic. Show that $f(x)$ is irreducible in $R[x]$ iff it is irreducible in $F[x]$.

Solution: This is known as Gauss's lemma.

a) By definition of integrality, α is a root of a monic polynomial $p(x) \in R[x]$. Let $m(x)$ be the minimal monic polynomial of α in $F[x]$. All of the other roots of m (in some algebraic closure of F) are roots of $p(x)$ (else we could take a gcd), so they are also integral over R. Hence the coefficients of m are also integral, since they are the symmetric functions of integral elements.

b) One direction is obvious: for the other, suppose $f(x)$ is irreducible in $R[x]$, and let $g(x) \in F[x]$ be monic, irreducible, and divide $f(x)$ in $F[x]$. If $\alpha \in \bar{F}$ is a root of $g(x)$ then since $g(x)$ is irreducible, $g(x)$ is the minimal polynomial of α. But since $f(\alpha) = 0$, α is integral over R, so by part (a) we see that $g(x) \in R[x]$, hence $g(x) = f(x)$ so we conclude f is irreducible.

---

14. (Jan-04.5) Let R be a ring with 1 and $V = X \oplus Y$ for nonzero (right) R-modules X and Y.

(a) Show that $0, X, Y, V$ are the only submodules of V iff X and Y are nonisomorphic simple R-modules.

(b) If X and Y are nonisomorphic simple R-modules, show that $\mathrm{End}_R(V)$ is isomorphic to the direct sum of two division rings.

Solution: Any submodule of X or Y gives a submodule of V, and furthermore, if $\phi : X \to Y$ is a nonzero homomorphism then $\{(x, \phi(x))\}$ is another submodule of V. Also note that if M is a simple module then every nonzero element is a generator, and also that if $\psi : M \to N$ is a nonzero homomorphism of simple modules then it is an isomorphism (as its kernel must be trivial and its image must be N).

a) By the above observation, if $0, X, Y, V$ are the only submodules then X and Y must be simple and nonisomorphic. Conversely, if X and Y are nonisomorphic and simple and A is any submodule of V, then consider the images of A projected into X and Y; since the images of the projections are submodules of X or Y, the projections are either zero or surjective. If both are zero then we have the 0 submodule, if one is zero then A is either a submodule of X or Y (hence A is X or Y). Now suppose neither is zero, and let $x \in X$ be nonzero and consider $y \in Y$ such that $(x, y) \in A$: if there are two such y, then $(x, y_1) - (x, y_2) = (0, y_1 - y_2) \in A$, so since $y_1 - y_2 \in Y$ is nonzero it generates Y, so $(0, y_1) \in A$ hence $(x, 0) \in A$ so all of X is in A, and similarly all of Y is in A, so $A = V$. Otherwise, for each $x \in X$ there is a unique $y \in Y$ such that $(x, y) \in A$: then $\phi : X \to Y$ sending each x to its corresponding y is a nonzero homomorphism hence an isomorphism, contradiction.

b) Let $\phi : V \to V$ and let $x \in X$ and $y \in Y$ be generators. We claim that $\phi(X) \subseteq X$ and $\phi(y) \subseteq Y$: since $\phi(X) \cong X/\ker(\phi)$ is either X or 0, we see that $\phi(X)$ must be either X or 0, since X is the only submodule of V isomorphic to X by part (a); similarly $\phi(Y) \subseteq Y$. Then $\mathrm{End}_R(V) \cong \mathrm{End}_R(X) \oplus \mathrm{End}_R(Y)$, and finally by Schur's lemma the endomorphism ring of a simple module is a division ring.
