Basic Notions in Algebra – Solutions to Ex. 5

Question 1.

(a) To prove that V_f is a submodule, note that if $v_1, v_2 \in V_f$ then $f(v_1+v_2) = f(v_1) + f(v_2) = 0$ by linearity of T. If $g \in F[x]$ then by commutativity of $F[x]$, if $v \in V_f$ then $f(gv) = g(fv) = 0$.

If $v = (x_0, x_1, \dots)$ and $f(t) = c_0 + c_1 t + \dots + c_n t^n$ where $c_n \neq 0$, it is easy to see that $fv = 0$ if and only if

$$c_0 x_t + c_1 x_{t+1} + \dots + c_n x_{t+n} = 0$$

for all $t \geq 0$. It follows (since $c_n \neq 0$) that the elements $x_n, x_{n+1}, \dots$ are *uniquely* determined by $x_0, \dots, x_{n-1}$. Since $x_0, \dots, x_{n-1}$ can be arbitrary, we get $\dim V_f = n = \deg f$.

(b) Write $g = hf$ where $h \in F[x]$. Then for any $v \in V_f$, $gv = h(fv) = 0$ hence $V_f \subseteq V_g$.

(c) Since $d = \gcd(f, g)$ divides both f and g, by (b) we have $V_d \subseteq V_f \cap V_g$. To prove the other inclusion, note that $F[x]$ is a PID (principal ideal domain), hence there are polynomials $a, b \in F[x]$ such that $d = af + bg$. It follows that if $v \in V_f \cap V_g$ then $dv = afv + bgv = 0$.

Since both f and g divide $l = \operatorname{lcm}(f, g)$, we have $V_f + V_g \subseteq V_l$. To prove the other inclusion, note that by unique factorization we always have $\gcd(f, g) \cdot \operatorname{lcm}(f, g) = f \cdot g$. In particular, $\deg d + \deg l = \deg f + \deg g$. But $\dim(V_f + V_g) = \dim V_f + \dim V_g - \dim(V_f \cap V_g) = \deg f + \deg g - \deg d = \deg l$. We deduce that $V_f + V_g$ is a subspace of V_l with the same dimension ($\deg l$), hence $V_f + V_g = V_l$.

(d) This follows from (c); if g_i are distinct irreducible then $\operatorname{lcm}(g_1^{e_1}, \dots, g_r^{e_r}) = g_1^{e_1} \dots g_r^{e_r}$ so that $V_f = \sum_{i=1}^r V_{g_i^{e_i}}$. But for all i, $V_{g_i^{e_i}} \cap \sum_{j \neq i} V_{g_j^{e_j}} = 0$ since $\gcd(g_i^{e_i}, \prod_{j \neq i} g_j^{e_j}) = 1$, hence the sum is direct.

(e) If f is not irreducible, find a non-trivial divisor g of f and then $V_g \subset V_f$ is a non-trivial submodule.

For the opposite direction, if $W \subset V_f$ is a submodule, by (g) there is a polynomial g such that $W = V_g$. Since $V_g = V_g \cap V_f = V_{\gcd(f,g)}$ it follows that g divides f. But f is irreducible hence g is either a scalar (so that $W = 0$) or a scalar multiple of f (so that $W = V_f$).

(f) If $f = g_1 \dots g_r$, semi-simplicity follows from the previous item. Conversely, we always have the decomposition $V_f = \oplus V_{g_i^{e_i}}$ where $f = g_1^{e_1} g_2^{e_2} \dots g_r^{e_r}$. To show that semi-simplicity implies $e_i = 1$ for all i, note that the only submodules of V_{g^2} for irreducible g are $0, V_g, V_{g^2}$ so it is not semi-simple.

(g) Since W is T-invariant, one can consider the restriction $T_{|W} : W \to W$. Now W is finite dimensional, so that the characteristic polynomial f_T of $T_{|W}$ is well-defined, and by the Cayley-Hamilton theorem, $f_T(T_{|W}) = 0$ on W. It follows that $f_T(T)_{|W} = 0$ so that $W \subseteq V_{f_T}$. But by the definition of the characteristic polynomial, $\dim V_{f_T} = \deg f_T = \dim W$, hence $W = V_{f_T}$.

(h) Follows from the previous items.

(i) Let $v_f \in V_f$ be the element whose first n coordinates are $0, 0, \ldots, 0, 1$ (and its next coordinates are determined by the recurrence f). Define a mapping $F[x] \to V_f$ by $g \mapsto g(v_f)$. It is easy to see that $v_f, xv_f, \ldots x^{n-1}v_f$ span V_f, hence this mapping is onto, or in other words $F[x]v_f = V_f$. In particular, V_f is *cyclic* and v_f is a cyclic vector in V_f.

Now if $gv_f = 0$, then for any $h \in F[x]$, $gh(v_f) = hg(v_f) = 0$, so that $g(V_f) = 0$. It follows that $V_f \subseteq V_g$ hence $f|g$. We deduce that the kernel of $g \mapsto g(v_f)$ is the ideal generated by (f) and the result follows by the isomorphism theorem.

(j) The definition of W should be the subspace *spanned* by all products vv' for $v \in V_f$, $v' \in V_g$.

Now if $v_1, \ldots, v_n$ and $u_1, \ldots, u_m$ are bases to V_f, V_g, the set of products $v_i u_j$ spans W, so W is finite dimensional. Since $T(v)T(v') = T(vv')$, it follows that W is T-invariant (because each V_f, V_g is, as a submodule). Therefore, by (g), there is a polynomial h such that $W = V_h$.

(k) From the formula one gets $\sqrt{F_n} = \sqrt{F_{n-1}} + \sqrt{F_{n-2}}$ (all elements are positive) and $\sqrt{F_0} = \sqrt{F_1} = 1$, so that $\sqrt{F_n}$ is the Fibonacci sequence. Now $F_n = \sqrt{F_n} \cdot \sqrt{F_n}$ is a product of linear recurring sequences and by (j) it is also a linear recurring sequence.

(l) Take $0 \subset V_x \subset V_{x^2} \subset \ldots$. Since $\dim V_{x^n} = n$ the sequence does not stop, so V does not have the maximum condition.

Let $g_1, g_2, \ldots$ be an infinite collection of irreducible polynomials (for example, there are irreducible polynomials of any degree), then

$$\bigoplus_{i=1}^{\infty} V_{g_i} \supset \bigoplus_{i=2}^{\infty} V_{g_i} \supset \bigoplus_{i=3}^{\infty} V_{g_i} \supset \ldots$$

is a decreasing sequence which does not stop (V_{g_n} is contained in the sum at the n-th step but not in the $n+1$-th step), so V does not have the minimum condition.

(m) For the maximum condition, take the same sequence as before. For the minimum condition, we note that any submodule of V_{x^∞} is V_{x^n} for some n or V_{x^∞}. Indeed, let W be such submodule and take $w \in W$. We have $w \in V_{x^n}$ for some n, so let $n_w = \inf\{n : w \in V_{x^n}\}$. Then $w \in V_{x^{n_w}} \setminus V_{x^{n_w - 1}}$. Since the only submodules of $V_{x^{n_w}}$ are V_{x^m} for $m \leq n_w$, it follows that the submodule generated by w is $V_{x^{n_w}}$, hence $V_{x^{n_w}} \subseteq W$.

Now consider $N = \sup_{w \in W} n_w$. If $N < \infty$ then by definition of n_w, $W \subseteq V_{x^N}$ so that $W = V_{x^n}$ for some n. If $N = \infty$, then by the above discussion $V_{x^n} \subseteq W$ for all n, hence $W = V_{x^\infty}$.

We deduce that a decreasing sequence of modules is either fixed at V_{x^∞} or has some element equal to V_{x^n}. In the latter case, the sequence must stop since V_{x^n} is finite dimensional.

Question 2.

(a) Let R be a finite domain and let $r \neq 0$ in R. Consider the mapping $R \to R$ defined by $a \mapsto ra$. This mapping is one-to-one, otherwise $r(a-b) = 0$ for $a \neq b$, contradicting the fact that R is a domain. Since R is finite, this mapping is also onto; in particular there exists a such that $ra = 1$.

(b) Such an idempotent e would satisfy $e(1-e) = 0$.

(c) If R is semi-simple which is not a division ring, then R is not simple, so there are non-trivial summands $R = S \oplus S'$. By previous exercise we get that there are non-trivial idempotents in $\mathrm{End}_R(R) \simeq R$.

(d) Combine the previous two items.

(e) A finite product of fields is semi-simple since a field is simple and a finite product is equal to the finite sum. Conversely, by the structure theorem a semi-simple ring R is a finite sum of matrix rings $M_{n_i}(\Delta_i)$ over division rings Δ_i. Since R is commutative, each summand $M_{n_i}(\Delta_i)$ must be commutative. It follows that $n_i = 1$ and Δ_i is commutative, so R is a finite product of fields.

Question 3.

(a) $\mathbb{Z}$ is not semi-simple by 2(d).

(b) The submodules of $\mathbb{Z}$ are its ideals, that is $n\mathbb{Z}$. They are not simple since $2n\mathbb{Z} \subset n\mathbb{Z}$. They are not semi-simple since they cannot be written as direct sums of ideals, because always $mn\mathbb{Z} \subseteq m\mathbb{Z} \cap n\mathbb{Z}$.

(c) $\mathbb{Z}$ does not satisfy the minimum condition: $\mathbb{Z} \supset 2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z} \supset \dots$

$\mathbb{Z}$ satisfies the maximum condition. Let $I_1 \subset I_2 \subset \dots$ be an increasing sequence of ideals. Let $I = \cup I_n$. Then I is an ideal, and since $\mathbb{Z}$ is PID, $I = (a)$ for some $a \in \mathbb{Z}$. But then $a \in I_n$ for some n, hence $(a) = I_n = I_{n+1} = \dots$.

(d) C_n is simple if and only if n is a prime. For if n is not prime, take $d|n$ a non-trivial divisor, and then $\{0, d, 2d, \dots\}$ is a non-trivial submodule of C_n. Conversely, C_p is a cyclic group of order p, hence any submodule (=subgroup) has order dividing p, so is either 0 or entire C_p.

By the Chinese Remainder Theorem, if $n = p_1^{e_1} \dots p_r^{e_r}$ (where p_i are distinct primes), $C_n = C_{p_1^{e_1}} \oplus \dots \oplus C_{p_r^{e_r}}$. It follows that if $e_i = 1$ for all i, then C_n is semi-simple. Conversely, if C_n is semi-simple, then $e_i = 1$ for all i. It is enough to verify that C_{p^2} is not semi-simple (because if $e_i > 1$ for some i, such module will be a submodule of C_n). This is clear since the subgroup $\{0, p, 2p, \dots, \}$ does not have a complement in C_{p^2}.

Same answer when C_n are considered as rings.

(e) Consider $\prod C_p$ where the product runs over all primes p. Then one has $\mathbb{Z} \subset \prod C_p$ through the diagonal embedding: $x \mapsto (x \mod p)_p$ (this is an embedding because an integer divisible by all primes is 0), but $\mathbb{Z}$ is not semi-simple, so $\prod C_p$ cannot be semi-simple (it contains a submodule which is not semi-simple).