Homework 3 Solutions

October 18, 2016

1. Let V be a finite-dimensional vector space over a field F. A linear transformation $T \in \mathrm{End}(V)$ is called *semisimple* if whenever W is an T-invariant subspace (that is $T(W) \subseteq W$) there exists a complementary T-invariant subspace W'. Here *complementary* means that $V = W \oplus W'$.

(a) If f is an irreducible polynomial in $F[x]$, let $V(f)$ be the subspace killed by a power of $f(T)$. Prove that V is the direct sum of the $V(f)$ as f runs over the irreducibles. Explain what this result has to do with the structure theory of finitely generated modules over a PID.

Remark: if F is algebraically closed, the irreducibles all have the form $f(x) = x - \lambda$ with $\lambda \in F$, and the $V(f)$ are called the *generalized eigenspaces*.

(b) Prove that T is semisimple if and only if its minimal polynomial m_T has no repeated irreducible factor.

(c) Let $n = \dim(V)$. Prove that $T^N = 0$ for some $N \geqslant 1$ if and only if $T^n = 0$. In this case T is *nilpotent*. Prove that with respect to some basis $v_1, \cdots, v_n$ the matrix of T is upper triangular, and indeed $Tv_i = v_{i-1}$ or $Tv_i = 0$.

(d) (**Jordan canonical form**) If $\lambda \in F$ the $k \times k$ *Jordan block* is the matrix

$$J_k(\lambda) = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix}.$$

Use (c) to show that over an algebraically closed field T may be written as a direct sum of Jordan blocks.

(e) (**Jordan decomposition**.) The linear transformation T is *unipotent* if $T - I_V$ is nilpotent. Assume that F is algebraically closed. Show that T may be written *uniquely* as $T_s T_u$ where T_s and T_u commute, with T_s semisimple and $T_u$we assume that unipotent.

Solution: (a) We make V into a module over the polynomial ring $F[X]$ by letting $f \in F[X]$ act on vectors via T:

$$f \cdot v = f(T)v, \qquad v \in V.$$

This is a torsion module, since V is finite dimensional. It is obviously finitely generated. Therefore we may invoke Theorem 7.5 on page 149 of Lang. It gives a decomposition

$$V = \bigoplus_{f \in F[V] \text{ irreducible}} V(f), \qquad V(f) = \{v \in V | f^N(T)v = 0, N \text{ large}\}.$$

(See the definition of $E(p)$ on page 149 of Lang.) This is exactly (a).

To prove (b) it will be useful to have the following simple but important fact, which is proved later in Lang's *Algebra*. Let R be a ring, and let M be an R-module. Then M is called *simple* if it is nonzero but has no proper nontrivial submodules. If R is a PID then it follows from the structure theory that every simple module is of the form $R/(f)$ where f is irreducible.

Proposition 1 *Let M be a module over a ring R. The following are equivalent.*

(1) If N is a submodule of M then there exists a submodule N' such that $M = N \oplus N'$.

(2) M is a direct sum of simple modules.

A module with either of these equivalent properties is called *semisimple*. Condition (1) is sometimes called *complete reducibility*.

Proof See Section 17.2 on page 645 of Lang for a prowe assume thatof of this equivalence. □

Making V into an $F[X]$-module as above, from criterion (1), V is semisimple as a module if and only if T is semisimple as an endomorphism. As before, we use Theorem 7.5 on page 149, write

$$V = \bigoplus_{f_i \in F[V] \text{ irreducible}} V(f_i), \qquad V(f_i) \cong \bigoplus_j R/f_i^{N_{ij}}).$$

The power of f_i that appears in the minimal polynomial is $\max_j(N_{ij})$, so no f_i appears with multiplcity greater than one if and only if all $N_{ij} = 1$ and this is also the condition for semisimplicity in condition (2).

[The next two exercises are from the end of Lang, Chapter 2, page 115.]

2. Let $\mathfrak{p}$ be a prime of the commutative ring A. Let $S = A - \mathfrak{p}$. Observe that S is a multiplicative set and consider $A_{\mathfrak{p}} = S^{-1}A$. Show that $A_{\mathfrak{p}}$ has a unique maximal ideal.

Solution. First we remind the reader about local rings. A ring is *local* if it has a unique maximal ideal.

Lemma 1 *If R is a commutative ring and $\mathfrak{m}$ is an ideal, then a necessary and sufficient condition for $\mathfrak{m}$ to be the unique maximal ideal of R is $R - \mathfrak{m}$ consists of the set of all units of R.*

Proof An element $\varepsilon \in R$ is a nonunit if and only if $R\varepsilon$ is a proper ideal, that is, if and only if ε is contained in a maximal ideal. So if $R - \mathfrak{m}$ consists of units, then every maximal ideal of R must be contained in $\mathfrak{m}$, implying that $\mathfrak{m}$ is the unique maximal ideal. The converse is similar. □

Consider $\mathfrak{p}A_{\mathfrak{p}} = \{p/s | p \in \mathfrak{p}, s \in S\}$. This is an ideal, with the property that its complement consists of units; indeed, if $a/s \in A_{\mathfrak{p}}$ is not in $\mathfrak{p}A_{\mathfrak{p}}$ then $a \notin \mathfrak{p}$, so $a \in S$ and therefore its inverse s/a is in $A_{\mathfrak{p}}$. We see that $A_{\mathfrak{p}} - \mathfrak{p}A_{\mathfrak{p}}$ consists of units, and the statement follows from the Lemma.

3. Show that if A is a principal ideal domain and S is a multiplicative set then $S^{-1}A$ is a principal ideal domain.

Solution. We identify $S^{-1}A$ with a subring of the field of fractions of A. Let $\mathfrak{A}$ be an ideal of $S^{-1}\mathfrak{A}$ and let $\mathfrak{a} = A \cap \mathfrak{A}$. Then $\mathfrak{a}$ is an ideal of A, so $\mathfrak{a} = Ax$ for some x because A is principal. Now clearly $S^{-1}A \cdot x \subseteq \mathfrak{A}$. Conversely if $a/s \in \mathfrak{A}$ then $a = s \cdot (a/s) \in \mathfrak{A} \cap A$ and therefore $a = bx$ for some b. Thus $a/s = (b/s)x \in S^{-1}A \cdot x$ We have proved that $\mathfrak{A}$ is principal generated by x.

4. Let $A = \mathbb{Z}[\sqrt{-5}]$ and $\mathfrak{p} = \{a + b\sqrt{-5} | a \equiv b \bmod 2\}$. Show that $\mathfrak{p}A_\mathfrak{p} = \alpha A_\mathfrak{p}$ where $\alpha = 1 + \sqrt{-5}$. Conclude that $A_\mathfrak{p}$ is a principal ideal domain with one nonzero prime ideal.

Solution. The ideal $\mathfrak{p}$ is clearly generated by α and 2. We have $2 = \frac{1}{3}\alpha\overline{\alpha} \in \alpha A_\mathfrak{p}$ since 3 is a unit in $A_\mathfrak{p}$. So $\mathfrak{p}A_\mathfrak{p} = 2A_\mathfrak{p} + \alpha A_\mathfrak{p} \subseteq \alpha A_\mathfrak{p} \subseteq \mathfrak{p}A_\mathfrak{p}$.

It remains to be shown that the local ring $A_\mathfrak{p}$ is a principal ideal domain. If this ring has nonprincipal ideals, then since it is Noetherian we can find an ideal $\mathfrak{a}$ that is maximal among the nonprinciple ideals. If $\mathfrak{a} = A_\mathfrak{p}$ then obviously $\mathfrak{a}$ is principal, so $\mathfrak{a}$ is proper. Since $\mathfrak{p}A_\mathfrak{p}$ is the unique maximal ideal of $A_\mathfrak{p}$ we have $\mathfrak{a} \subseteq \mathfrak{p}A_\mathfrak{p} = \alpha A_\mathfrak{p}$ and therefore $\alpha^{-1}\mathfrak{a} \subseteq A_\mathfrak{p}$. Because $\alpha^{-1}\mathfrak{a}$ is a submodule of $A_\mathfrak{p}$ it is an ideal.

We will show that $\alpha^{-1}\mathfrak{a}$ is strictly larger than $\mathfrak{a}$. We have $\alpha\mathfrak{a} \subseteq \mathfrak{a}$ since $\alpha \in A_\mathfrak{p}$ and so $\alpha^{-1}\mathfrak{a} \supseteq \mathfrak{a}$. If it is not strictly larger than $\mathfrak{a}$ then α^{-1} is integral over $A_\mathfrak{p}$ by the condition Int 3 on page 334. This means that we have an integral equation:

$$\alpha^{-N} + c_{N-1}\alpha^{-(N-1)} + \cdots + c_0 = 0, \qquad c_i \in A_\mathfrak{p}.$$

That means that $\alpha^{-1} = -(c_{N-1} + c_{N-2}\alpha + \ldots + c_0\alpha^N) \in A_\mathfrak{p}$. This is impossible since $\alpha \in \mathfrak{p}A_\mathfrak{p}$ lies in the maximal ideal, hence cannot be a unit.

Now $\alpha^{-1}\mathfrak{a}$ is strictly larger than $A_\mathfrak{p}$ and by maximality of $\mathfrak{a}$ this ideal is principal, say $\alpha^{-1}\mathfrak{a} = (\beta)$. Then $\mathfrak{a} = (\alpha\beta)$ is principal, which is a contradiction.

A principal ideal domain that is local, i.e. has only one nonzero prime ideal is called a *discrete valuation ring* (DVR), an important class of rings. This example illustrates the fact that localizing a Dedekind domain gives a DVR.