Homework 6 Solutions

The goal of the first problem is to prove the Artin-Rees Lemma, which was stated without proof in *Dimension II* and applied to the Krull Dimension Theorem.

Problem 1. Let A be a Noetherian commutative ring, $\mathfrak{a}$ an ideal, and M a finitely-generated A-module. Let $R = A[x]$ be the polynomial ring and $M[x]$ the R-module of polynomials $\sum_i m_i x^i$ with $m_i \in M$.

$$R' = \left\{ \sum_{k=0}^{m} a_k x^k \in R | a_k \in \mathfrak{a}^k \right\}, \qquad M' = \left\{ \sum_{k=0}^{n} m_k x^k | m_k \in \mathfrak{a}^k M \right\}$$

(i) Prove that R' is a Noetherian ring and M' a finitely generated R'-module.
(ii) Let N be a submodule of M. Let $N' = \left\{ \sum_{k=0}^{n} m_k x^k | m_k \in N \cap \mathfrak{a}^k M \right\}$. Show that N' is a finitely generated R'-module, and deduce the Artin-Rees Lemma.

Solution. (i) Since R is Noetherian, $\mathfrak{a}$ is finitely generated. Let $a_1, \cdots, a_r$ be generators. Then R' is the ring generated by $a_i x$, since any element of $\mathfrak{a}^n$ is spanned by elements of the form $a_{i_1} \cdots a_{i_n}$, so $\mathfrak{a}^k x^k$ is spanned by elements $(a_{i_1} x) \cdots (a_{i_n} x)$. Since R' is thus a finitely-generated algebra over the Noetherian ring A, it is Noetherian by the Hilbert basis theorem. Similarly M' is generated by elements $a_i m_i x$. As a finitely-generated submodule over a Noetherian ring, M' is finitely generated as an R'-module.

(ii) Note that $R'N' \subseteq N'$, so N' is an R'-submodule of R'. Since R' is Noetherian, N' is finitely generated.

Let us deduce the Artin-Rees Lemma, which asserts that there exists an r such that $\mathfrak{a}^n M \cap N = \mathfrak{a}^{n-r}(\mathfrak{a}^r M \cap N)$ when $n \geqslant r$. The inclusion $\mathfrak{a}^{n-r}(\mathfrak{a}^r M \cap N) \subseteq \mathfrak{a}^n M \cap N$ is clear. To prove the other inclusion, let $n_{i_1} x^{i_1}, \cdots, n_{i_k} x^{i_k}$ be generators of N' as an R'-module, and let $r = \max(i_1, \cdots, i_k)$. Now suppose that $n \geqslant r$. We will show that $\mathfrak{a}^n M \cap N = \mathfrak{a}^{n-r}(\mathfrak{a}^r M \cap N)$. Indeed, let $\eta \in \mathfrak{a}^n M \cap N$. Then $\eta x^k \in N'$ so we may write ηx^k as a linear combination of elements $\xi(n_{i_k} x^{i_k})$ where $\xi \in \mathfrak{a}^{n-i_k} x^{i_k}$. Now

$$\xi(n_{i_k}) \in \mathfrak{a}^{n-i_k}(\mathfrak{a}^{i_k} M \cap N) = \mathfrak{a}^{n-r} \cdot \mathfrak{a}^{r-i_k}(\mathfrak{a}^{i_k} M \cap N) \subseteq \mathfrak{a}^{n-r}(\mathfrak{a}^r M \cap N)$$

because $\mathfrak{a}^{r-i_k}(\mathfrak{a}^{i_k} M \cap N) \subseteq \mathfrak{a}^r M \cap N$. This proves the Artin-Rees Lemma.

Now let A be a commutative ring and M an A-module. Define a topology on M in which a subset $U \subseteq M$ is open if and only if for every $x \in U$, the set U contains $x + \mathfrak{a}^n M$ for some n. Thus a sequence $x_i \longrightarrow 0$ if and only if for every n, $x_i \in \mathfrak{a}$ for sufficiently large i. This is called the $\mathfrak{a}$–adic topology on M. This leads to the $\mathfrak{a}$-*adic completion* $\hat{M}$ whose use is a powerful technique for studying M.

Problem 2. Assume that A is Noetherian, and let M a finitely generated $\mathfrak{a}$-module with the $\mathfrak{a}$-adic topology. Let N be a submodule of M. We have two topologies on N: its own $\mathfrak{a}$-adic topology, and its subspace topology as a submodule of M. Show that these two topologies are the same.

Hint: Use the Artin-Rees Lemma.

Solution. Let U be a subset of N. To be open in the $\mathfrak{a}$-adic topology on N, we need to know that if $a \in U$ then $a + \mathfrak{a}^n N \subseteq U$ for some n. On the other hand to be open in the induced topology we need to know that $a + (\mathfrak{a}^m M \cap N) \subset U$ for some m. Clearly

$$a + (\mathfrak{a}^n M \cap N) \subset U \qquad \Rightarrow \qquad a + \mathfrak{a}^n N \subset U.$$

To prove the converse, note that $\mathfrak{a}^{n+r} M \cap N = \mathfrak{a}^n(\mathfrak{a}^r M \cap N) \subseteq \mathfrak{a}^n N$ so

$$a + \mathfrak{a}^n N \subset U \qquad \Rightarrow \qquad a + (\mathfrak{a}^{n+r} M \cap N) \subset U.$$

Representations

If M is a module for the group algebra $\mathbb{C}[G]$ of a finite group, and $g \in G$, we define an endomorphism $\pi(g) : M \longrightarrow M$ by $\pi(g)v = g \cdot v$. This is a representation of G. Conversely, given a representation $\pi : G \longrightarrow \mathrm{GL}(M)$, where M is a complex vector space, then M admits the structure of a $\mathbb{C}[G]$-module by

$$\left(\sum_{g \in G} a_g g\right) \cdot v = \sum a_g \pi(g)(v), \qquad v \in M.$$

In these notes we will always assume that the module M is *finite-dimensional.* The *character* of M is the character of the corresponding representation. So

$$\chi(g) = \mathrm{tr}\ \pi(g).$$

If V is a vector space, a map $p : V \longrightarrow V$ is called a *projection* if $p^2 = p$.

Problem 3. Let G be a finite group, $R = \mathbb{C}[G]$ its group algebra. If M is an R-module, let

$$M^G = \{x \in M | gx = x \text{ for all } g \in G\}$$

be the module of invariants. Define the endomorphism $p : M \longrightarrow M$ by

$$p(v) = \frac{1}{|G|} \sum_{g \in G} g \cdot v. \tag{1}$$

Prove that p is a projection map whose image is M^G and deduce that

$$\dim(M^G) = \frac{1}{|G|} \sum_{g \in G} \chi(g).$$

Solution. Step 1: the image of p is contained in M^G. Indeed, if $g \in G$ then

$$g \cdot p(v) = g \cdot \frac{1}{|G|} \sum_{h \in G} h \cdot v = \frac{1}{|G|} \sum_{h \in G} (gh) \cdot v.$$

Making the variable change $h \mapsto g^{-1}h$, this becomes

$$\frac{1}{|G|} \sum_{h \in G} g \cdot v = p(v).$$

We have shown $g \cdot p(v) = p(v)$ so $p(v) \subseteq M^G$.

Step 2: if $v \in M^G$ then $p(v) = v$. Indeed, each term in the sum (1) equals v, so $p(v) = v$.

Step 3: $p^2 = p$. Indeed, if $v \in M$ then $p(v) \in M^G$ by Step 1, so $p(p(v)) = p(v)$ by Step 2. Therefore $p^2 = p$.

Step 4: $M = \ker(p) \oplus \mathrm{im}(p)$. (This is true for any projection and was proved in class on February 16.) Indeed, we have $\ker(p) \cap \mathrm{im}(p) = 0$ because if $x \in \ker(p) \cap \mathrm{im}(p)$, write $x = p(y)$ because $x \in \mathrm{im}(p)$, then note that $x = p(y) = p^2(y) = p(x) = 0$ because $x \in \ker(p)$. Moreover $M = \ker(p) + \mathrm{im}(p)$ since any $x \in M$ may be written $x = (x - p(x)) + p(x)$ where $x - p(x) \in \ker(p)$ and $p(x) \in \mathrm{im}(p)$. This proves that $M = \ker(p) \oplus \mathrm{im}(p)$.

Let $d = \dim(M^G) = \mathrm{im}(p)$ and let $n = \dim(M)$. Choose a basis for M such that the first d basis vectors $x_1, \cdots, x_d$ are in M^G and the remaining basis vectors $x_{d+1}, \cdots, x_n$ are in $\ker(p)$. With respect to this basis, the matrix of p is the block diagonal matrix

$$\begin{pmatrix} I_d & \\ & 0_{n-d} \end{pmatrix}$$

so its trace is $d = \dim(M^G)$. Therefore, in terms of the corresponding representation π and its character χ:

$$\dim(M^G) = \mathrm{tr}(p) = \frac{1}{|G|} \sum_{g \in G} \mathrm{tr}\ \pi(g) = \frac{1}{|G|} \sum_{g \in G} \chi(g)$$

Problem 4. Let M and N be $\mathbb{C}[G]$-modules. Let $W = \mathrm{Hom}_{\mathbb{C}}(M, N)$ be the space of linear transformations $T : M \longrightarrow N$. Show that W has the structure of a $\mathbb{C}[G]$-module such that

$$(g\phi)(x) = g \cdot \phi(g^{-1} \cdot x), \qquad x \in M.$$

Show that the character of W is $\chi_M(g^{-1})\chi_N(g)$, where χ_M and χ_N are the characters of M and N.

Solution. Choose bases for M and N as vector spaces. Thus if $m = \dim(M)$ and $n = \dim(N)$ we identify $\mathrm{GL}(M) = \mathrm{GL}_m(\mathbb{C})$, $\mathrm{GL}(N) = \mathrm{GL}_n(\mathbb{C})$ and

$$\mathrm{Hom}_{\mathbb{C}}(M, N) = \mathrm{Mat}_{m \times n}(\mathbb{C}).$$

The representations $\pi_M : G \longrightarrow \mathrm{GL}(M) = \mathrm{GL}_m(\mathbb{C})$ and $\pi_N : G \longrightarrow \mathrm{GL}(N) = \mathrm{GL}_n(\mathbb{C})$ coming from the $\mathbb{C}[G]$-module structures on M and N are realized in terms of matrices.

Let E_{ij} be the basis element of $\mathrm{Mat}_{m\times n}(\mathbb{C})$ having 1 in the i,j position and 0 elsewhere. Now let $A=(a_{ij})\in \mathrm{GL}_m(\mathbb{C})$ and $B=(b_{ij})\in \mathrm{GL}_n(\mathbb{C})$ and consider the linear transformation Φ of $\mathrm{Mat}_{m\times n}(\mathbb{C})$ such that $\Phi(T)=BTA$. It follows from the definition of matrix multiplication that

$$\Phi(E_{ij})=b_{ii}a_{jj}E_{ij}+\text{linear combination of other } E_{kl}.$$

So taking the trace picks off the diagonal, and

$$\mathrm{tr}(\Phi)=\sum_{i,j} b_{ii}a_{jj}=\mathrm{tr}(A)\,\mathrm{tr}(B).$$

We apply this with $A=\pi_M(g^{-1})$ and $B=\pi_N(g)$.

Problem 5. Let F be a field of characteristic p, and let $G=\langle\sigma\rangle$ a cyclic group of order p generated by $\sigma\in G$. Let R be the group algebra $F[G]$. Show that R has elements $\tau_1,\cdots,\tau_p$ such that

$$\begin{aligned}\sigma\tau_1 &= \tau_1,\\ \sigma\tau_i &= \tau_i-\tau_{i-1}\quad (i>1).\end{aligned}$$

Describe all ideals of R and deduce that R is not a semisimple ring.

Solution. Let

$$\tau_1=1+\sigma+\sigma^2+\ldots+\sigma^{p-1},$$
$$\tau_2=1+2\sigma+3\sigma^2+\cdots+(p-1)\sigma^{p-2}$$

and in general

$$\tau_k=\sum_{j=0}^{p-k}\binom{k+j-1}{k-1}\sigma^j.$$

The last case $k=p$ has only one term $j=0$ so

$$\tau_p=1.$$

It is evident that $\sigma\tau_1=\tau_1$. If $k>1$ we have

$$\tau_k-\sigma\tau_k=\sum_{j=0}^{p-k}\binom{k+j-1}{k-1}\sigma^j-\sum_{j=0}^{p-k}\binom{k+j-1}{k-1}\sigma^{j+1}$$

$$=\sum_{j=0}^{p-k}\binom{k+j-1}{k-1}\sigma^j-\sum_{j=1}^{p-k+1}\binom{k+j-2}{k-1}\sigma^j \qquad (2)$$

To compute the coefficient of σ^j we have to handle the cases $j = 0$ and $j = p - k + 1$ separately. Leaving these aside for the moment assume that $1 \leqslant j \leqslant p - k$. Then the coefficient of σ^j is

$$\binom{k+j-1}{k-1} - \binom{k+j-2}{k-1} = \binom{k+j-2}{k-2} \tag{3}$$

due to the Pascal triangle identity

$$\binom{a}{b} + \binom{a}{b+1} = \binom{a+1}{b+1},$$

If $j = 0$, there is only a contribution to σ^j from the first sum in (2) and that coefficient is 1, which also agrees with $\binom{k+j-2}{k-2}$. Finally, if $j = p - k + 1$ there is a contribution from the second sum in (2), and that contribution is $-\binom{k+p-k+1-2}{k-1} = -\binom{p-1}{k-1}$. Now in characteristic p we have

$$-\binom{p-1}{k-1} = \binom{p-1}{k-2}$$

since

$$\binom{p-1}{k-2} + \binom{p-1}{k-1} = \binom{p}{k-1} \equiv 0 \mod p.$$

We see that in every case the coefficient of σ^j is $\binom{k+j-2}{k-2}$ so

$$\tau_k - \sigma\tau_k = \sum_{j=1}^{p-k+1} \binom{k+j-2}{k-2} = \tau_{k-1}.$$

Now we may determine the ideals of $F[G]$. From the identity $\sigma\tau_i = \tau_i - \tau_{i-1}$ it is clear that

$$I_k = F\tau_1 \oplus \cdots \oplus F\tau_k$$

is closed under the action of G, hence is an ideal. We claim that these are all the ideals of $F[G]$. Define a degree function δ on the nonzero elements of $F[G]$ by declaring $\delta(\phi)$ to be the largest k such that $a_k \neq 0$ when we write $\phi = \sum a_k\tau_k$. From the fact that $\tau_k - \sigma\tau_k = \tau_{k-1}$ we have

$$\deg(\phi - \sigma\phi) = \deg(\phi) - 1 \tag{4}$$

provided $\deg(\phi) > 1$. Let I be an ideal and choose $\phi \in I$ of maximal degree k. From (4) we see that I has elements of every degree $\leqslant k$. These are linearly independent and span I_k, so $I = I_k$.

The ring is not semisimple because I_k is not complemented by any ideal J such that $F[G] = I_k \oplus J$. This is clear since we know all the ideals of $F[G]$.