Math 101 Fall 2013
Homework #4
Due Wednesday October 16, 2013

1. Let $R = \mathbf{Q}[x]$ and let V be the 2-dimensional rational vector space $\mathbf{Q}^2$ and let $T : V \to V$ be given by $Tv = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} v$. View V as a R-module in the usual way $p(x) \cdot v = p(T)v$. Let $u = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $v = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Find $|u|$ and $|v|$.

> **ANS**: Since $Tu = u$, $(x-1) \cdot u = 0$. Since $u \neq 0$ and $\deg x - 1 = 1$, we must have $|u| = x - 1$. On the other hand, $Tv = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. It then follows immediately that $(x-a) \cdot v \neq 0$ for any a. Hence the order of v must be a polynomial of degree at least 2. But a simple computation shows that $(x^2 - 2x + 1) \cdot v = 0$. Hence $|v| = (x-1)^2$.

2. Let M be a module over a PID. Suppose that x and y are torsion elements in M with orders r and s, respectively. If $(r, s) = 1$, then show that the order of $x + y$ is rs.

> **ANS**: Let a and b be such that $as + br = 1$. Since $rs \cdot (x + y) = 0$, the order t of $x + y$ divides rs. But if $t \cdot (x + y) = 0$, then $t \cdot x = -t \cdot y$. Then $tr \cdot y = 0$ and $s \mid tr$. But $as + br = 1$ implies $ast + brt = t$. Hence $s \mid t$. Similarly $r \mid t$. But then $ast + brt = t$ implies that $rs \mid t$. Thus rs and t are associates.

3. Show that a ring R is Noetherian if and only if every ideal in R is finitely generated. In this problem R is any ring. Ideal means two-sided ideal, and Noetherian means every ascending sequence of ideals is eventually constant.

> **ANS**: Suppose every ideal in R is finitely generated. Let $I_1 \subset I_2 \subset \cdots$ be an ascending sequence if ideals. Let $I = \bigcup I_i$. Then I is an ideal. Say that I is generated by $x_1, \ldots, x_k$. But for some N, $n \geq N$ implies all the x_i are in I_n. But then we clearly have $I = I_n$ for all $n \geq N$.
>
> On the other hand, let I be an ideal in R which is not finitely generated. Let $x_1 \in I \setminus \{0\}$. Then the ideal, (x_1), generated by x_1 can't be all of I. So pick $x_2 \in I \setminus (x_1)$. Continue. Then $(x_1) \subset (x_1, x_2) \subset \cdots$ is an ascending sequence of ideals which is not eventually constant.

4. Suppose that R is a PID. The aim of this problem is to prove the special case of Hilbert's Theorem which says that $R[x]$ is a Noetherian ring. Let I be a nonzero ideal in $R[x]$. By question 3, it will suffice to show that I is finitely generated. For each $n \geq 0$, let A_n be the union of the zero element and all elements of R which occur as leading coefficients of polynomials of degree n in I. (Thus $a_n \in A_n \setminus \{0\}$ if and only if there is a $p(x) \in I$ of the form $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$.)

(a) Show that each A_n is an ideal in R and that $A_n \subset A_{n+1}$ for all $n \geq 0$.

(b) Conclude that there is an r such that $A_n = A_r$ for all $r \geq n$.

(c) Since R is a PID, we have $A_n = (a_n)$ and there is a degree n polynomial $p_n(x)$ in I with leading coefficient a_n. Let J be the ideal in $R[x]$ generated by $\{p_0(x), \dots, p_r(x)\}$. Then given any polynomial $f(x)$ of degree d in I, that there a polynomial $g(x) \in J$ such that the degree of $f(x) - g(x)$ is strictly less than d.

(d) Conclude that $I = J$. Hence I is finitely generated.

ANS: (a) Suppose that a and b are in $A_n \setminus \{0\}$. Then there are degree n polynomials $f(x)$ and $g(x)$ with leading coefficients a and b, respectively. If $b = -a$, then $a + b = 0 \in A_n$ by definition. Otherwise, $f(x) + g(x)$ has degree n and $a + b \in A_n$. If $r \in R$, then either $r = 0$, or $r \cdot f(x) \in I$ and has degree n. In any event, $ra \in A_n$. Thus A_n is an ideal. On the other hand, the leading coefficient of $xf(x)$ is still a, so $A_n \subset A_{n+1}$. This proves (a).

(b) Since R is a PID, it is Noetherian.

(c) In this problem, as suggested in lecture, it is convenient to assign degree -1 to the zero polynomial. Let $f(x)$ be a polynomial in I with degree $d \geq 0$. If $d > r$, then the leading coefficient of $f(x)$ is ca_r for some $c \in R$. Then $f(x) - x^{d-r}p_r(x)$ has degree strictly less than d and of course $x^{d-r}p_r(x) \in J$. On the other hand, if $\deg f(x) = k \leq r$, then the leading coefficient of $f(x)$ is of the form ca_k where $A_k = (a_k)$. Then $f(x) - cp_k(x)$ has degree strictly less than $d = k$. Again, $cp_k(x) \in J$.

(d) We claim that if $f(x) \in I$, then $f(x) \in J$. This will suffice. This is clear if $f(x) = 0$ (or if $f(x)$ is constant). We assume the result if $\deg f(x) < d$. Clearly, $J \subset I$. But by the previous part, there is a $g(x) \in J$ such that $f(x) - g(x)$ is in I and has degree strictly less than d. Hence $f(x) - g(x) \in I$ by assumption. Since $g(x) \in I$, this means $f(x) \in I$, and we are done.

5. Let M be a module over a PID R. Suppose that $m \in M$ has order r. If $s \in R$, show that $\langle m \rangle[s] = \langle \frac{r}{(r,s)} \cdot m \rangle \cong R/(r, s)$. (Here "$(r, s)$" is used both to designate the ideal generated by r and s as well as the generator of that ideal.)

ANS: Note that $\left(\frac{r}{(r,s)}, \frac{s}{(r,s)}\right) = 1$. Also, you should be able to prove that if $(a, b) = 1$ and $a \mid bc$, then $a \mid c$. Using these observations we have

$$\begin{aligned}
\langle m \rangle[s] &= \{\, u \cdot m : su \cdot m = 0 \,\} \\
&= \{\, u \cdot m : r \mid su \,\} \\
&= \{\, u \cdot m : \frac{r}{(r,s)} \mid \frac{s}{(r,s)} u \,\} \\
&= \{\, u \cdot m : \frac{r}{(r,s)} \mid u \,\} \\
&= \langle \frac{r}{(r,s)} \cdot m \rangle.
\end{aligned}$$

Thus we get a map of R onto $\langle m \rangle$ by $v \mapsto \frac{vr}{(r,s)} \cdot m$, and this map clearly has kernel (r, s). Thus the isomorphism claimed in the problem follows from the First Isomorphism Theorem for Modules.

6. Let F be a field and give $R = \prod_{n=1}^{\infty} F$ the obvious ring structure. Let $I = \{\, (x_i) \in R : x_i = 0$ for all by finitely many $i\,\}$.

(a) Observe that I is an ideal in R. Hence I is an R-module.

(b) Show that I is not a finitely generated R-module.

(c) Conclude that submodules of finitely generated modules need not be finitely generated.

ANS: This is the example Michael suggested in lecture. Parts (a) and (c) are straightforward; it is easy to see that I is an ideal and R is generated by its identity (the constant function 1).

For part (b), suppose the contrary that I were generated as an R-module by $m_1, \dots, m_k$. Then for each i there is an N_i such that $n \geq N_i$ implies that $m_i(n) = 0$. Let $N = \max\{N_1, \dots, N_k\}$. Then if m is the "linear combination" $r_1 \cdot m_1 + \cdots + r_k \cdot m_k$ for $r_i \in R$, then $m(n) = 0$ for all $n \geq N$. But the submodule generated by $\{m_1, \dots, m_k\}$ consists precisely of all such linear combinations. Hence $\epsilon_N \notin \langle\{m_1, \dots, m_k\}\rangle$. This shows I can't be finitely generated.

7. Here and elsewhere, V_T is the $F[x]$-module corresponding to a finite-dimensional F-vector space V and linear map $T : V \to V$. Suppose that $W = \langle v \rangle$ is a cyclic submodule of V_T of order $f(x)$ for $f \in F[x]$ with $\deg f = k > 0$. Show that $\{v, Tv, T^2v, \dots, T^{k-1}v\}$ is a (vector space) basis for W.

ANS: Note that the map $p(x) \mapsto p(x) \cdot v$ factors through an isomorphism of $F[x]/(f(x))$ onto W. Since $f(x)$ has degree k, every element of $F[x]/(f(x))$ has a representative of the form $[b_0 + b_1x + \cdots + b_{k-1}x^{k-1}]$: by the division algorithm, every $g(x) \in F[x]$ is of the form $q(x)f(x) + r(x)$ with $\deg r(x) < k$. (In fact, it is not so hard to see that $F[x]/(f(x))$ is an F-vector space of dimension k.) Hence it is clear that $\beta = \{v, Tv, T^2v, \dots, T^{k-1}v\}$ spans W. On the other hand if $c_0v + c_1Tv + \cdots + c_{k-1}T^{k-1}v = 0$, then $g(x) \cdot v = 0$ where $g(x) = c_0 + c_1x + \cdots c_{k-1}x^{k-1}$. But f is the nonzero polynomial of minimal degree such that $f(x) \cdot v = 0$. Hence $g(x)$ is the zero polynomial and all the c_i are zero. Thus β is linearly independent and spans; that is, β is a basis as claimed.