MATH 437: Homework III.
Due in class on Friday, Feb 13

1. **[Representing homomorphisms of free modules.]**
Let R be a ring with $1 \neq 0$ (not necessarily commutative) and let F be a free R-module with a basis $\{\hat{e}_1, \ldots, \hat{e}_n\}$ of size n. (This exercise also goes thru for infinite basis but we will stick to the finite dimensional case for ease of notation.)

Given $\hat{w} \in F$ we may write $\hat{w}$ uniquely as $\hat{w} = \sum_{i=1}^n w_i \hat{e}_i$. Thus we may represent $\hat{w}$ uniquely as a column vector $\begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix}$ where the $w_i \in R$ are the "components of $\hat{w}$" with respect to the basis $\{\hat{e}_1, \ldots, \hat{e}_n\}$.

Now if $S : F \to F$ is an R-module endomorphism, we may define scalars $a_{ij} \in R, 1 \leq i, j \leq n$ by the identity:

$$S(\hat{e}_j) = \sum_{i=1}^n a_{ij} \hat{e}_i.$$

Finally it will be useful to introduce the concept of the opposite ring $R^{op} = (R, +, \star)$ to a given ring $R = (R, +, \cdot)$. As an Abelian group under $+$, $R^{op} = R$, however the multiplication is given by $r \star s = s \cdot r$ for all $r, s \in R$. Note that if R is commutative then $R^{op} = R$.
(a) Show that $S(\hat{w}) = \sum_{i=1}^n (\sum_{j=1}^n w_j a_{ij}) \hat{e}_i = \sum_{i=1}^n (\sum_{j=1}^n a_{ij} * w_j) \hat{e}_i$.

What this calculation shows is that if we let $\mathbb{A}_S$ be the matrix whose (i, j)-entry is a_{ij} then the column vector representing $S(\hat{w})$ is obtained by matrix multiplication

$$\mathbb{A}_S \star \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix}$$

in the "opposite ring" R^{op}. Thus we say the matrix $\mathbb{A}_S$ represents the endomorphism $S : F \to F$.
(b) Show that the correspondence $S \to \mathbb{A}_S$ induces an isomorphism between the rings $Hom_R(F, F)$ and $Mat_n(R^{op})$. (In particular you should show composition of endomorphisms corresponds to matrix multiplication

of the corresponding representing matrices when the entries are viewed in R^{op}. Here the matrix multiplication $\mathbb{A}\mathbb{B}$ is defined via the usual formula $(\mathbb{A}\mathbb{B})_{ij} = \sum_{k=1}^{n} a_{ik} \star b_{kj}$ from linear algebra.)
(c) Fix a field k and consider the polynomial ring $F = k[x_1, \ldots, x_n]$. Check that F is free as a $R = k[x_1, \ldots, x_{n-1}]$-module, with basis $\{x_n^k | k = 0, 1, 2, \ldots\}$. We define formal differentiation with respect to x_n as the R-module endomorphism $\frac{\partial}{\partial x_n}$ of F given uniquely by the condition

$$\frac{\partial(x_n^k)}{\partial x_n} = kx_n^{k-1}$$

for $k = 0, 1, 2, \ldots$. Find the kernel of $\frac{\partial}{\partial x_n}$ (be careful to consider the characteristic of k) and also write down the matrix representing $\frac{\partial}{\partial x_n} : F \to F$ with respect to the given basis.

2. **[I-adic metrics]** Fix a real number $0 < \alpha < 1$ thruout this problem. As usual we adopt the conventions $\alpha^0 = 1$ and $\alpha^\infty = 0$.

(a) Let R be any ring and I be a two-sided ideal of R and set $I^0 = R$.
We define the I-adic pseudometric $d_I(r, s) = \alpha^{sup_{n \in \mathbb{N}}\{r - s \in I^n\}}$.
Show that this is a non-Archimedean pseudometric on R, i.e.,

$$d_I(r, s) \geq 0 \text{ for all } r, s \in R$$
$$d_I(r, s) = d_I(s, r) \text{ for all } r, s \in R \text{ and}$$
$$d_I(r, s) \leq max\{d_I(r, z), d_I(z, s)\} \text{ for all } r, s, z \in R.$$

Note that the final condition which is called the non-Archimedean property implies the usual triangle inequality and is a stronger condition in general. Also note that this pseudometric is translation invariant, i.e., $d_I(r+z, s+z) = d_I(r, s)$. The word pseudometric is used as it is possible that $d_I(r, s) = 0$ but $r \neq s$ in general.
Show that d_I defines a metric on R whenever $\cap_{n=1}^{\infty} I^n = 0$.
Describe $B_{d_I}(0, \epsilon) = \{r \in R | d_I(r, 0) < \epsilon\}$ in terms of I for all $\epsilon > 0$.
(b) Review the concepts of convergence, Cauchy sequences and dense sets from metric space theory. Recall that a metric space is complete if every Cauchy sequence converges.

Show that in a non-Archimedean metric space, a sequence $\{x_n | n \in \mathbb{N}\}$ is Cauchy if and only if for every $\epsilon > 0$, there exists a N_ϵ such that $d(x_n, x_{n+1}) < \epsilon$ for all $n > N_\epsilon$. (Note: The condition is not the definition of a Cauchy

sequence as this requires a control of $d(x_n, x_m)$ for all sufficiently high m, n. In an arbitrary metric space, the condition would not be equivalent.)
(c) Note that the Krull Intersection Theorem shows that d_J defines a metric on R when R is a commutative Noetherian ring and J is the Jacobson radical of R. Now consider the power series ring $k[[x]]$ where k is a field. Recall $J = (x)$. Given two power series f and g **give a simple description** of $d_J(f, g)$ in terms of the coefficients of f and g.
Show that $(k[[x]], d_J)$ is a complete metric space.
Show that the polynomial ring $k[x]$ is dense inside of $(k[[x]], d_J)$.
(d) Show that the polynomials $f_N = \prod_{n=1}^{N}(1 + x^n)$ form a Cauchy sequence in $(k[[x]], d_J)$ and hence that they converge to a power series f. f is usually denoted as $\prod_{n=1}^{\infty}(1 + x^n)$. Can you find the first 9 terms in the power series expansion of f?
(e) Let $R = \mathbb{Z}$ and let p be a prime number. Check that $d_{(p)}$ is a metric on $\mathbb{Z}$. Calculate $d_{(p)}(20, 32)$ for all primes p (in terms of α).

$d_{(p)}$ is called the p-adic metric on $\mathbb{Z}$. Usually one sets $\alpha = \frac{1}{p}$ when using the p-adic metric but this is not essential. We will see later that $(\mathbb{Z}, d_{(p)})$ is not a complete metric space.

3. [**I-adic completions**] Fix a real number $0 < \alpha < 1$ as before.
An inverse system $\{R_n | n \in \mathbb{N}\}$ of rings is a collection of rings R_n and ring homomorphisms $\phi_n : R_{n+1} \to R_n$ for each $n \in \mathbb{N}$. Given such an inverse system, the inverse limit $\underset{\leftarrow}{Lim} R_n$ is the subset of the direct product $\times_{n \in \mathbb{N}} R_n$ consisting of tuples $(r_n)_{n \in \mathbb{N}}$ of compatible elements. More precisely,

$$\underset{\leftarrow}{Lim} R_n = \{(r_n)_{n \in \mathbb{N}} \in \prod_{n \in \mathbb{N}} R_n | \phi_n(r_{n+1}) = r_n \text{ for all } n \in \mathbb{N}\}.$$

[This is a special kind of inverse system and inverse limit, there is a more general theory of inverse limits of which this is the most important example - see Lang.]
(a) Check that $\underset{\leftarrow}{Lim} R_n$ is a subring of $\times_{n \in \mathbb{N}} R_n$. The projections $\pi_j : \times_{n \in \mathbb{N}} R_n \to R_j$ restrict to projections $\pi_j : \underset{\leftarrow}{Lim} R_n \to R_j$. Show that

$$d(\hat{r}, \hat{s}) = \alpha^{sup\{n \in \mathbb{N} | \hat{r} - \hat{s} \in ker(\pi_j) \text{ for all } j \leq n\}}$$

is a metric on $\underset{\leftarrow}{Lim} R_n$. This is called the canonical metric on the inverse limit.

(b) Given a two-sided ideal I of R, note that $R_n = R/I^n$ are rings with canonical quotient homomorphisms $\phi_n : R/I^{n+1} \to R/I^n$ between them.

The inverse limit $\underset{\leftarrow}{Lim}(R/I^n)$ of this inverse system is called the ***I*-adic completion** of R and is denoted $\hat{R}_I$ or just $\hat{R}$ if the ideal I is understood.

Show that the map $\lambda : R \to \hat{R}_I$ given by $\lambda(r) = (r + I^n)_{n\in\mathbb{N}}$ is a well-defined homomorphism of rings with kernel equal to $\cap_{n\in\mathbb{N}} I^n$.

(c) By (b), when $\cap_{n\in\mathbb{N}} I^n = 0$, R embeds inside of $\hat{R}_I$ as the "constant sequences". Show that in this case, the canonical metric d on the inverse limit $\hat{R}_I$ when restricted to R gives the I-adic metric d_I on R. Furthermore show that any Cauchy sequence in (R, d_I) converges in $(\hat{R}_I, d)$. Finally show that R is dense in $\hat{R}_I$, that is arbitrarily close to any "compatible sequence" lies a "constant sequence". These three things show that $(\hat{R}_I, d)$ is a metric space completion of (R, d_I).

(d) When $R = \mathbb{Z}$ and $I = (p)$ where p is a prime, the completion $\hat{\mathbb{Z}}_{(p)}$ is called the p-adic integers and is usually just denoted by $\hat{\mathbb{Z}}_p$.

For any formal expression $\sum_{n=0}^{\infty} a_i p^i$ where $0 \leq a_i < p$, show that the sequence of integers $Z_N = \sum_{n=0}^{N} a_i p^i$ is a Cauchy sequence in $(\mathbb{Z}, d_{(p)})$. Conclude that the sequence $\{Z_N\}_{N\in\mathbb{N}}$ hence converges to a unique $Z \in \hat{\mathbb{Z}}_p$. Thus $\sum_{n=0}^{\infty} a_i p^i$ defines a unique p-adic integer in this way.

It turns out with a little work, one may also show the converse, i.e., that every p-adic integer is given by such an expansion and hence develop a picture of p-adic integers as formal series in p. The integers then correspond to the "polynomials in p".

(e) Let $f \in \hat{\mathbb{Z}}_p[x]$ be a polynomial. Show that the map $x \to f(x)$ is a continuous map on $\hat{\mathbb{Z}}_p$. (In the canonical metric of $\hat{\mathbb{Z}}_p$)

4. **[One variable Hensel's Lemma]** Let $f(x) \in \mathbb{Z}[x]$ and let p be a prime of $\mathbb{Z}$.

(a) Show that for every $a \in \mathbb{Z}$, there exists a polynomial $h_a(x) \in \mathbb{Z}[x]$ such that $f(a + x) = f(a) + f'(a)x + h_a(x)x^2$. Here f' is the derivative of f.

(b) Suppose p does not divide an integer γ, show that the map $\theta_\gamma : \mathbb{Z}/p^{k+1}\mathbb{Z} \to \mathbb{Z}/p^{k+1}\mathbb{Z}$ given by $\theta_\gamma(m) = \gamma m$ is an isomorphism of abelian groups.

(c) Let $k \geq 1$. Suppose $a_k \in \mathbb{Z}$ is a nonsingular approximate root of f in the sense that $f(a_k) \equiv 0 \bmod p^k$ and p does not divide $f'(a_k)$. Show that there exists an integer a_{k+1} such that

$$f'(a_k)(a_{k+1} - a_k) \equiv -f(a_k) \bmod p^{k+1}.$$

Show that $a_{k+1} \equiv a_k \bmod p^k$, $f(a_{k+1}) \equiv 0 \bmod p^{k+1}$ and that p does not divide $f'(a_{k+1})$.

Note that this shows that a_{k+1} is a "better" nonsingular approximate root of $f(x)$ in the sense that $d_{(p)}(f(a_{k+1}), 0) < d_{(p)}(f(a_k), 0)$.

(d) Show that if $f \in \mathbb{Z}[x]$ has a nonsingular root $\bar{a}_1 \in \mathbb{F}_p$, i.e., $f(a_1) \equiv 0 \bmod p$ and $f'(a_1) \not\equiv 0 \bmod p$ then one can construct a sequence of integers $\{a_n | n \in \mathbb{Z}\}$ which converge in $\hat{\mathbb{Z}}_p$ (in the canonical metric) to a p-adic root of f, i.e., an $a \in \hat{\mathbb{Z}}_p$ with $f(a) = 0$.

(e) Let p be an odd prime. Show that $x^2 + 1$ has a p-adic root if and only if $p \equiv 1 \bmod 4$. (Hint: First decide when $x^2 + 1$ has a root in $\mathbb{F}_p$ by analyzing the multiplicative order of such a root.)

Remark: Hensel's Lemma is the basis of finding p-adic solutions to polynomial equations once one has found a $\mathbb{F}_p$ solution say by an exhaustive search. Since $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}_p$, it is a "folklore principle" called the Hasse principle that once one has a $\hat{\mathbb{Z}}_p$ solution for all primes p to the equation, it is likely there is an integer solution. Finding the integer solutions to a given polynomial equation is in general very hard - think Fermat's Last Theorem!