# MATH 603: HOMEWORK #3

DUE IN SEBASTIAN MOORE'S MAILBOX BY 4:00 P.M., FEB. 22

## 1. Rational and Jordan canonical forms

1. Find the rational canonical form of the matrix

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 3 & 6 \\ 0 & 0 & 5 \end{pmatrix}. \tag{1.1}$$

in $\mathrm{Mat}_3(\mathbb{Q})$.

2. Suppose $F$ is a field and $\lambda, \lambda' \in F$. When are the matrices

$$A = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} \lambda' & 0 & 0 \\ 1 & \lambda' & 0 \\ 0 & 1 & \lambda' \end{pmatrix} \tag{1.2}$$

conjugate in $\mathrm{GL}_3(F)$? Explain your answer.

## 2. Cohen-Lenstra statistics

Let $p$ be a prime and let $[B]$ be the isomorphism class of a finite abelian $p$ group $B$. In class we discussed the idea, going back to H. Cohen and H. W. Lenstra, Jr., that if one chooses a finite abelian $p$-group $A$ "at random," the probability $\mu([B])$ that $A$ will land in the isomorphism class $[B]$ should be proportional to $1/\#\mathrm{Aut}(B)$. Write $\mu([B]) = c/\#\mathrm{Aut}(B)$ for some constant $c$. Let $S$ be the set of all isomorphism class of finite abelian $p$-groups. Then

$$\sum_{[B]\in S} \mu([B]) = c \sum_{[B]\in S} \frac{1}{\#\mathrm{Aut}(B)} \quad \text{so} \quad \frac{1}{c} = \sum_{[B]\in S} \frac{1}{\#\mathrm{Aut}(B)}.$$

The object of this exercise is to compute $c$. We will regard $A$ and $B$ as modules for the localization $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ at $(p) = \mathbb{Z}p$. Note that $\mathbb{Z}_{(p)}$ is a discrete valuation ring, so that it is Euclidean and a P.I.D..

0. Show that a finite abelian group $C$ is a $\mathbb{Z}_{(p)}$-module if and only if $C$ has order a power of $p$.

1. Suppose $A$ and $B$ are finitely generated $\mathbb{Z}_{(p)}$-modules, and that $A$ is generated by $\le n$ elements. Define

$$\mathrm{Hom}^{sur}_{\mathbb{Z}_{(p)}}(A, B) = \{f \in \mathrm{Hom}_{\mathbb{Z}_{(p)}}(A, B) : f \text{ is surjective}\}$$

$$\lambda_n(A) = \#\{N \subset \mathbb{Z}^n_{(p)} : [\mathbb{Z}^n_{(p)}/N] = [A]\} \quad \text{if} \quad A \quad \text{is finite}$$

$$s_n(A) = \#\mathrm{Hom}^{sur}_{\mathbb{Z}_{(p)}}(\mathbb{Z}^n_{(p)}, A) \quad \text{if} \quad A \quad \text{is finite.} \tag{2.1}$$

Show that $\#\mathrm{Aut}(A) \cdot \lambda_n(A) = s_n(A)$ if $A$ is finite.

2. Suppose $A$ is a finite abelian $p$ group. Then $A/pA$ is a finite vector space over $\mathbb{Z}/p$; let $r = \nu(A)$ be the rank of this vector space. Show that for $n \geq \nu(A)$, a homomorphism $f : \mathbb{Z}_{(p)}^n \to A$ is surjective if and only if the induced homomorphism
$$\overline{f} : \frac{\mathbb{Z}_{(p)}^n}{p \cdot \mathbb{Z}_{(p)}^n} \to \frac{A}{pA} \cong (\mathbb{Z}/p)^r$$
is surjective. Conversely, show that if one is given a surjection $\overline{f}$ of this kind, it arises from a surjection $f : \mathbb{Z}_{(p)}^n \to A$. Show that in this case, if $g : \mathbb{Z}_{(p)}^n \to A$ is any other homomorphism for which $\overline{g} = \overline{f}$, then $g = f + h$ for a unique homomorphism $h \in \mathrm{Hom}_{\mathbb{Z}_{(p)}}(\mathbb{Z}_{(p)}^n, pA)$. Show that the number of such $h$ is $(\#pA)^n$.

3. Show that the elements of $\mathrm{Hom}^{surj}((\mathbb{Z}/p)^n, (\mathbb{Z}/p)^r)$ can be identified with $r \times n$ matrices with entries in $\mathbb{Z}/p$ with column rank $r$, in the sense that the span of the columns has dimension $r$ over $\mathbb{Z}/p$. By picking $r$ linearly independent columns, show these matrices are exactly the ones with row rank $r$. Then show that with the hypotheses of problem # 2, one has
$$\begin{aligned} s_n(A) &= \left(\#\mathrm{Hom}^{surj}_{\mathbb{Z}_{(p)}}((\mathbb{Z}/p)^n, (\mathbb{Z}/p)^r)\right) \cdot \left(\#\mathrm{Hom}(\mathbb{Z}_{(p)}^n, pA)\right) \\ &= (p^n - 1) \cdot (p^n - p) \cdots (p^n - p^{r-1}) \cdot (\#pA)^n \\ &= (\#A)^n \frac{(q)_n}{(q)_{n-r}} \end{aligned} \tag{2.2}$$
where for $i \geq 0$,
$$q = p^{-1} \quad \text{and} \quad (q)_i = \prod_{j=1}^{i} (1 - q^j) \quad \text{and} \quad r = \nu(A).$$

4. Let $T(n)$ be the set of all isomorphism classes $[M]$ of finite abelian $p$ groups for which $\nu(M) = n$, i.e. for which the minimal number of generators for $M$ is $n$. Define
$$S(n) = \sum_{[M] \in T(n)} \frac{1}{\#\mathrm{Aut}(M)}$$
so that
$$\frac{1}{c} = \sum_{\text{all } [M]} \frac{1}{\#\mathrm{Aut}(M)} = \sum_{n=0}^{\infty} S(n).$$
Use problem 2 to show that
$$S(n) = \sum_{U \subset p\mathbb{Z}_{(p)}^n} s_n(\mathbb{Z}_{(p)}^n / U)^{-1}$$
when $s_n(A)$ is defined as in (2.1) and $U$ runs over all finite index subsets of $p\mathbb{Z}_{(p)}^n$. Then use (2.2) to show
$$S(n) = \sum_{U \subset p\mathbb{Z}_{(p)}^n} [\mathbb{Z}_{(p)}^n : U]^{-n} \frac{1}{(q)_n} = \frac{q^{n^2}}{(q)_n} \zeta(\mathbb{Z}_{(p)}^n, n) \tag{2.3}$$
Here
$$\zeta(\mathbb{Z}_{(p)}^n, s) = \sum_U [\mathbb{Z}_{(p)}^n : U]^{-s}$$
is the zeta function considered in homework set #2, where $U$ ranges over all the finite index submodules of $\mathbb{Z}_{(p)}^n$. Recall that that in that homework assignment you showed
$$\zeta(\mathbb{Z}_{(p)}^n, n) = \prod_{j=0}^{n-1} (1 - p^{j-n})^{-1}.$$

5. Deduce that
$$\frac{1}{c} = \sum_{\text{all } [M]} \frac{1}{\#\mathrm{Aut}(M)} = \sum_{n=0}^{\infty} \frac{q^{n^2}}{(q)_n^2}$$

**Extra Credit** Show that $\frac{1}{c}$ in problem #5 equals
$$\frac{1}{c} = \frac{1}{(q)_\infty} = \frac{1}{\prod_{j=1}^{\infty}(1-q^j)}.$$

## 3. Fine moduli spaces

Let $\mathcal{C}$ be a full subcategory of the category of all Noetherian affine schemes $\mathrm{Spec}(A)$ over a ring $R$. Here $A$ is a Noetherian $R$-algebra, the morphisms $\tau : \mathrm{Spec}(A) \to \mathrm{Spec}(A')$ correspond to $R$-algebra homomorphsms $A' \to A$. The condition that $\mathcal{C}$ is full means that if $\mathrm{Spec}(A)$ and $\mathrm{Spec}(A')$ are objects in $\mathcal{C}$ then all scheme morphisms $\tau$ between them over $R$ are morphisms in $\mathcal{C}$.

A set valued contravariant functor $\mathcal{L} : \mathcal{C} \to \mathrm{Sets}$ has an affine fine moduli scheme $\mathrm{Spec}(D)$ if $D$ is an $R$-algebra and there is an isomorphism of functors between $\mathcal{L}$ and the functor which sends $\mathrm{Spec}(A) \in \mathrm{Objects}(\mathcal{C})$ to the set $\mathrm{Mor}_R(\mathrm{Spec}(A), \mathrm{Spec}(D))$ of all $R$-scheme morphisms from $\mathrm{Spec}(A)$ to $\mathrm{Spec}(D)$.

1. Suppose $A$ and $A'$ are $R$-algebras. Let $A \oplus A'$ be their direct sum. Show that $\mathrm{Spec}(A \oplus A')$ is the disjoint union of $\mathrm{Spec}(A)$ and $\mathrm{Spec}(A')$. Show if $B$ is an $R$-algebra which is an integral domain, the morphisms from $\mathrm{Spec}(B)$ to $\mathrm{Spec}(A \oplus A')$ are the disjoint union of the morphisms from $\mathrm{Spec}(B)$ to $\mathrm{Spec}(A)$ and to $\mathrm{Spec}(A')$, respectively. (Hint: Consider the orthogonal idempotents $(0,1)$ and $(1,0)$ in $A \oplus A'$). Can you drop the condition that $B$ is an integral domain?
2. Suppose $R$ is a field $F$ and that $L$ is a field containing $F$. The affine space of dimension $n$ over $F$ is the scheme $\mathbb{A}^n_F = \mathrm{Spec}(F[x_1, \ldots, x_n])$ in which $x_1, \ldots, x_n$ are commuting indeterminates. Show that the set $\mathrm{Mor}_F(\mathrm{Spec}(L), \mathbb{A}^n_F)$ of $F$-morphisms from $\mathrm{Spec}(L)$ to $\mathbb{A}^n_F$ is identified with the set of $n$-tuples $z_1, \ldots, z_n$ of elements of $L$.
3. Let $R$ be a field $F$, and let $\mathcal{C}$ be the category of affine schemes over $F$ of the form $\mathrm{Spec}(L)$ for some field $L$ containing $F$. Fix an integer $d \geq 1$. Define $\mathcal{L} : \mathcal{C} \to \mathrm{Sets}$ to be the contravariant functor which sends $\mathrm{Spec}(L)$ to the set of isomorphism classes $[(V, T)]$, where $V$ is a $d$-dimensional vector space over $L$ and $T : V \to V$ is an $L$-linear map. Here another pair $(V', T')$ defines the same isomophism class $[(V', T')] = [(V, T)]$ if there is an $L$-linear isormorphism $V \to V'$ which carries $T$ to $T'$. Show that $\mathcal{L}$ has a fine moduli scheme which is a disjoint union of affine spaces.

   (Hint: Show that if $a_1(x), \ldots, a_n(x)$ are monic polynomials in $L[x]$ with $a_1(x)|\cdots|a_n(x)$, then there are unique monic polynomials $c_i(x)$ for $i = 1, \ldots, n-1$ such that $a_{i+1}(x) = a_i(x)c_i(x)$. Now consider the coefficients of $a_1(x)$ and $c_i(x)$ for $i = 1, \ldots, n-1$.)