Algebra 4 (2004-05) – Assignment 3

Instructor: Dr. Eyal Goren

Submit by Monday, January 31, 24:00 by mail-box on 10^{th} floor.

1) Let $f : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ be a group homomorphism represented with respect to the standard basis by a matrix $M \in M_n(\mathbb{Z})$. Assume that $\det(M) \neq 0$. Prove that

$$\sharp(\mathbb{Z}^n / f(\mathbb{Z}^n)) = |\det(M)|.$$

2) Let $\mathbb{F}$ be a field and $A \in M_n(\mathbb{F})$. We think of A as defining an $\mathbb{F}[x]$ module structure on $\mathbb{F}^n$. Note that the structure theorem says that there is a basis for $\mathbb{F}^n$ in which multiplication by x is given by $\operatorname{diag}(C_{a_1(x)}, C_{a_2(x)}, \dots, C_{a_m(x)})$, where $a_1(x)|a_2(x)|\dots|a_m(x)$ are the invariant factors and the $C_{a_i(x)}$ the companion matrices. That means that if we let N be the change of basis matrix then $NAN^{-1} = \operatorname{diag}(C_{a_1(x)}, C_{a_2(x)}, \dots, C_{a_m(x)})$. Note that if for some other basis with change of basis matrix N' we have that $N'AN'^{-1} = \operatorname{diag}(C_{a'_1(x)}, C_{a'_2(x)}, \dots, C_{a'_{m'}(x)})$ with $a'_1(x)|a'_2(x)|\dots|a'_{m'}(x)$ then this gives a decomposition of the $\mathbb{F}[x]$ module $\mathbb{F}^n$ into a direct sum of modules of the form $\mathbb{F}[x]/(a'_i(x))$ and thus (if all polynomials considered are monic) we have $m = m'$ and $a_i(x) = a'_i(x)$ for all i. Namely, A is equivalent to a unique block matrix of companion matrices associated to polynomials that divide each other in the manner described above. We call $a_1(x), \dots, a_m(x)$ also the invariant factors of A.

(1) Prove that two matrices A and B in $M_n(\mathbb{F})$ are similar, i.e. there is an invertible matrix $C \in M_n(\mathbb{F})$ such that $CAC^{-1} = B$, if and only if A and B has the same invariant factors. (This is quite easy.)

(2) Let $\mathbb{F}$ be a finite field with q elements; let $\mathrm{GL}_n(\mathbb{F})$ act on $M_n(\mathbb{F})$ by $(C, A) \mapsto CAC^{-1}$. Write a formula for the number of orbits of this action for $n = 1, 2, 3, 4, 5, 6$.
Guidance: I don't think the Cauchy-Frobenius formula is of any help in this case. I suggest using the statement in (1). After doing those cases (you can explain in detail the cases $n = 2, 3$ and just compute the rest) you'll be able to write a general "formula" that holds for every n.