Math 210B Algebra: Homework 6

March 15th, 2019

Professor Sharifi

Anish Chedalavada

Exercise 1. *Find a set of representatives for the similarity classes of matrices $A \in \mathbb{M}_2(\mathbb{F}_{19})$ with $A^5 = I$.*

Proof. We have that $19 \equiv 4 \mod 5$ has multiplicative order 2, and so $[\mathbb{F}_{19}(\zeta_5) : \mathbb{F}_{19}] = 2$. Thus, consider the polynomial $p = (t-\zeta_5)(t-\zeta_5^2)(t-\zeta_5^3)(t-\zeta_5^4) \in \mathbb{F}_{19}[t]$. The minimal polynomial of any root divides p and must be degree 2, so we may assume the irreducible factors of this polynomial in $\mathbb{F}_{19}[t]$ are $(t-\zeta_5)(t-\zeta_5^4)$ and $(t-\zeta_5^2)(t-\zeta_5^3)$ (as for any other product $(t-\zeta_5)(t-\zeta_5^n)$ the constant term does not belong in $\mathbb{F}_{19}$). Thus, the irreducible factors of t^5-1 are $(t-\zeta_5)(t-\zeta_5^4)$, $(t-\zeta_5^3)(t-\zeta_5^2)$, $(t-1)$. Thus, for any $A \in \mathbb{M}_2(\mathbb{F}_{19})$ with $q_A \mid t^5 - 1$ and $\deg q_A \leq 2$, the minimal polynomial of A is either $(t-\zeta_5)(t-\zeta_5^4)$, $(t-\zeta_5^3)(t-\zeta_5^2)$ or $(t-1)$, and so the representatives (by rational canonical form) are:

$$\begin{pmatrix} 0 & -1 \\ 1 & \zeta_5 + \zeta_5^4 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & \zeta_5^2 + \zeta_5^3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

□

Exercise 2. *Let $A \in GL_n(\mathbb{C})$ with minimal and characteristic polynomial $(x-\lambda)^n$. Find the Jordan Canonical Forms of all A^k with $k \geq 1$.*

Proof. In Jordan Canonical Form, A may be represented as:

$$\begin{pmatrix} \lambda & & 0 \\ & \ddots & \\ 0 & & \lambda \end{pmatrix} + N_n$$

For N_n representing the nilpotent element of order n in $\mathbb{M}_n(\mathbb{C})$:

$$N_n = \begin{pmatrix} 0 & & & 0 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & 0 \end{pmatrix}$$

As these matrices commute with each other, we have a binomial expansion for A^k, given by:

$$A^k = \begin{pmatrix} \lambda^k & & 0 \\ & \ddots & \\ 0 & & \lambda^k \end{pmatrix} + k \begin{pmatrix} \lambda^{k-1} & & 0 \\ & \ddots & \\ 0 & & \lambda^{k-1} \end{pmatrix} N_n + \binom{k}{2} \begin{pmatrix} \lambda^{k-2} & & 0 \\ & \ddots & \\ 0 & & \lambda^{k-2} \end{pmatrix} N_n^2 + \dots + N_n^k$$

We know that the above matrix is lower triangular, with progressive binomial coefficients on the lower off diagonals. This gives us that the characteristic polynomial is $(t^k - \lambda^k)^n$. Let $d < n$. Then $(A^k - \lambda^k I)^d$ is given by the sum below:

$$(A^k - \lambda^k)^d = k \begin{pmatrix} \lambda^{dk-d} & & 0 \\ & \ddots & \\ 0 & & \lambda^{dk-d} \end{pmatrix} N_n^d + \dots$$

But here it is clear that all other terms will contain powers of N_{n-1} greater than d, and so are sums of matrices with values in the entries strictly below the off diagonal associated to N_{n-1}^d, and so are linearly independent to it. Thus, $(A^k - \lambda^k I)^d = 0$ only when $d \geq n$, as all the terms contain powers of N_n greater than or equal to n. Thus, the minimal and characteristic polynomials of A^k are $t^k - \lambda^k$ and so it has Jordan form:

$$\begin{pmatrix} \lambda^k & & & 0 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & \lambda^k \end{pmatrix}$$

□

Exercise 3. *Let $a, b \in \mathbb{Q}$. Express $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(a + b\zeta_5)$ and $Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(a + b\zeta_5)$ as sums of rational numbers.*

Proof. We have $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(a + b\zeta_5) = (a + b\zeta_5)(a + b\zeta_5^2)(a + b\zeta_5^3)(a + b\zeta_5^4)$. Using the fact that $(1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4) = 0$, an application of the additive Satz 90, we may apply the reduction:

$$\begin{aligned}
&(a + b\zeta_5)(a + b\zeta_5^2)(a + b\zeta_5^3)(a + b\zeta_5^4) = (a^2 + ab(\zeta_5 + \zeta_5^4) + b^2)(a^2 + ab(\zeta_5^2 + \zeta_5^3) + b^2) \\
&= (a^4 + (a^3b + ab^3)(\zeta_5^2 + \zeta_5^3 + \zeta_5 + \zeta_5^4) + a^2b^2(\zeta_5^2 + \zeta_5^3)(\zeta_5 + \zeta_5^4) + 2a^2b^2 + b^4) \\
&= (a^4 + (a^3b + ab^3)(\zeta_5^2 + \zeta_5^3 + \zeta_5 + \zeta_5^4) + a^2b^2(\zeta_5^2 + \zeta_5^3)(\zeta_5 + \zeta_5^4) + 2a^2b^2 + b^4) \\
&= (a^4 - (a^3b + ab^3) + a^2b^2(\zeta_5^3 + \zeta_5^4 + \zeta_5 + \zeta_5^2 + 1) + a^2b^2 + b^4) \\
&= (a^4 - a^3b + a^2b^2 - ab^3 + b^4) = \frac{(a^5 + b^5)}{a + b}
\end{aligned}$$

And so $N_{\mathbb{Q}(\zeta)/\mathbb{Q}}(a + b\zeta_5) = \frac{(a^5+b^5)}{a+b}$. Expanding the trace yields: $Tr_{\mathbb{Q}(\zeta)/\mathbb{Q}}(a + b\zeta_5) = (a + b\zeta_5) + (a + b\zeta_5^2) + (a + b\zeta_5^3) + (a + b\zeta_5^4) = 5a - b$. □

Exercise 4. *Let L/K be an extension of finite fields. Show that both $N_{L/K} : L^\times \to K^\times$ and $Tr_{L/K} : L \to K$ are surjective maps.*

Proof. Hilbert's Theorem 90 tells us that the kernel of the norm map is of the form $\frac{\sigma(a)}{a}$ for some $\sigma \in G(L/K)$. As $\sigma(a) = a$ for any $a \in K$, we have that $N_{L/K}|_{K^\times}$ has trivial kernel, and any endomrophism of a finite field with trivial kernel must be surjective. An analogous argument applies for the norm map, except now on the additive group. □

Exercise 5. *Let F be a field, $a \in F$.*
a. For $n \geq 1$, find the discriminant of $x^n - a$.
b. For characteristic p, calculate the discriminant of $x^p - x - a$.

Proof. a. We may assume the polynomial is separable, as if it were not then the discriminant would be 0. The discriminant may be computed as:

$$\begin{aligned}
&(-1)^{\frac{n(n-1)}{2}} \prod_i (f'(\alpha_i)) = (-1)^{\frac{n(n-1)}{2}} (n\sqrt[n]{a^{n-1}})...(n\sqrt[n]{a^{n-1}}\zeta_5^{(n-1)(n-1)}) \\
&= n^n a^{n-1} \prod_i (\zeta_5^{in-i}) = na^{n-1}
\end{aligned}$$

b. For the Artin-Schreier polynomial, we have that the roots are of the form $\{\alpha, \alpha + 1, ..., \alpha + p - 1\}$. Computing the discriminant for this yields:

$$\begin{aligned}
&(-1)^{\frac{p(p-1)}{2}} \prod_{a \neq b \in \mathbb{Z}/p\mathbb{Z}} (\alpha + b - \alpha - a) = (-1)^{\frac{p(p-1)}{2}} \prod_{a \neq b \in \mathbb{Z}/p\mathbb{Z}} (b - a) \\
&= (-1)^{\frac{p(p-1)}{2}} \left(\prod_{a \in (\mathbb{Z}/p\mathbb{Z})^\times} a \right)^p = (-1)^{\frac{p(p-1)}{2}} (-1)^p = (-1)^{\frac{p(p+1)}{2}}
\end{aligned}$$

With the last step made by Wilson's Theorem. □

Exercise 6. *Let p be a prime number, and let ζ_p be a primitive pth root of unity Set $F = \mathbb{Q}(\zeta_p)$. Find a necessary and sufficient condition on $a \in F^\times - F^{\times p}$ s.t. $K = F(a^{1/p})$ is Galois over $\mathbb{Q}$, and under that condition, determine $G(K/\mathbb{Q})$, explicitly a semidirect product of two cyclic groups.*

Proof. It is both necessary and sufficient that a^k We have the perfect Kummer pairing:

$$G(K/F) \times < a > \to \mu_m$$

$G(K/F) = \mathbb{Z}/p\mathbb{Z}$ □