Zhengdong Zhang
Email: zhengz@uoregon.edu
Course: MATH 649 - Abstract Algebra
Instructor: Professor Sasha Polishchuk

Homework - Week 4
ID: 952091294
Term: Spring 2025
Due Date: 30^{th} April , 2025

Problem 12.16
Let char $k \neq 2$ and $f \in \Bbbk[x]$ be a cubic whose discriminant has a square root in $\Bbbk$, then f is either irreducible or splits in $\Bbbk$.

Solution: Let $\mathbb{K}$ be the splitting field of f over $\Bbbk$. First we suppose f has multiple roots. Then the discriminant $\Delta(f) = 0$ has a square root in $\Bbbk$. If f has only one root α, then f is irreducible when $\alpha \notin \Bbbk$ and f splits in $\Bbbk$ when $\alpha \in \Bbbk$. If α as a root of f has multiplicity 2, let β be another root of f, $f(x)$ can be written as

$$f(x) = (x-\alpha)^2(x-\beta)$$

when $\beta \in \Bbbk$, we know that $(x-\alpha)^2 = x^2 - 2\alpha x + \alpha^2 \in \Bbbk[x]$. Note that 2 is invertible in $\Bbbk$, so this implies $\alpha \in \Bbbk$. Thus, f splits in $\Bbbk$. When $\alpha \in \Bbbk$, it is easy to see that $\beta \in \Bbbk$ and f again splits in $\Bbbk$. If neither α nor β is in $\Bbbk$, then f is irreducible over $\Bbbk$.

Now suppose f does not have multiple roots. By Theorem 12.1.2, the Galois group $G = \mathrm{Gal}(\mathbb{K}/\Bbbk) \leq A_3 \cong C_3$. We know that C_3 is simple and only have two subgroups: $\{e\}$ or C_3. When $G = \{e\}$, this means $\mathbb{K} = \Bbbk$, so f splits in $\Bbbk$. When $G = C_3$, this means the action of G on the roots of f is transitive, thus f is irreducible.

Problem 12.4.9
Let $\mathbb{K}/\Bbbk$ be a finite Galois extension and $\alpha \in \mathbb{K}$. Consider the $\Bbbk$-linear operator $A_\alpha : x \mapsto \alpha x$ on the $\Bbbk$-vector space $\mathbb{K}$. Then $\det A_\alpha = N_{\mathbb{K}/\Bbbk}(\alpha)$ and $\mathrm{tr}\ A_\alpha = T_{\mathbb{K}/\Bbbk}(\alpha)$.

Solution: Let $p(x) \in \Bbbk[x]$ be the minimal polynomial of α over $\Bbbk$ and $\deg p = d$. $p(x)$ has d roots $\alpha_1, \alpha_2, \ldots, \alpha_d$ where $\alpha = \alpha_1$. Suppose $[\mathbb{K} : \Bbbk] = n$ and $r := \frac{n}{d}$. We prove $\det A_\alpha$ and $N_{\mathbb{K}/\Bbbk}(\alpha)$ are both equal to $(\alpha_1\alpha_2\cdots\alpha_d)^r$, and both $\mathrm{tr}\ A_\alpha$ and $T_{\mathbb{K}/\Bbbk}(\alpha)$ are equal to $r(\alpha_1 + \cdots + \alpha_d)$.

(1) In this part we prove that

$$\begin{aligned} \det A_\alpha &= (\alpha_1 \cdots \alpha_d)^r, \\ \mathrm{tr}\ A_\alpha &= r(\alpha_1 + \cdots + \alpha_d). \end{aligned}$$

Let $\Bbbk(\alpha)$ be the splitting field of p. Suppose

$$p(x) = (x-\alpha_1)\cdots(x-\alpha_d) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

$\Bbbk(\alpha)$ as a $\Bbbk$-vector space has a basis $\left\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\right\}$. The multiplication of α in $\Bbbk(\alpha)$ can be written as a matrix

$$B = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d-1} \end{pmatrix}$$

The determinant of this matrix B is $(-1)^{d-1} \cdot (-a_0) = (-1)^d a_0$ and the trace of this matrix B is $-a_{d-1}$. Note that in $p(x)$, we have

$$(x - \alpha_1) \cdots (x - \alpha_d) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

By comparing coefficients, we notice that

$$\begin{aligned} (-1)^d(\alpha_1 \cdots \alpha_d) &= a_0, \\ -(\alpha_1 + \cdots + \alpha_d) &= a_{d-1} \end{aligned}$$

This proves that $\det B = \alpha_1 \cdots \alpha_d$ and tr $B = \alpha_1 + \cdots + \alpha_d$. Now consider the extension $\mathbb{K}/\Bbbk(\alpha)/\Bbbk$, we have

$$[\mathbb{K} : \Bbbk(\alpha)] = \frac{[\mathbb{K} : \Bbbk]}{[\Bbbk(\alpha) : \Bbbk]} = \frac{n}{d} = r.$$

Choose $\{\beta_1, \ldots, \beta_r\}$ as a $\Bbbk(\alpha)$-basis of $\mathbb{K}$. Then

$$\begin{gathered} \beta_1, \alpha\beta_1, \ldots, \alpha^{d-1}\beta_1, \\ \beta_2, \alpha\beta_2, \ldots, \alpha^{d-1}\beta_2, \\ \cdots \\ \beta_r, \alpha\beta_r, \ldots, \alpha^{d-1}\beta_r. \end{gathered}$$

is a $\Bbbk$-basis for $\mathbb{K}$. Note that multiplicating by α only sends a base vector to linear combinations of the basis in the same row. So the matrix A_α is a block matrix with r block each equal to B. Thus,

$$\begin{aligned} \det A_\alpha &= (\det B)^r = (\alpha_1 \cdots \alpha_d)^r, \\ \text{tr } A_\alpha &= r(\text{tr } B) = r(\alpha_1 + \cdots + \alpha_d). \end{aligned}$$

(2) In this part we prove that

$$\begin{aligned} N_{\mathbb{K}/\Bbbk}(\alpha) &= (\alpha_1 \cdots \alpha_d)^r, \\ T_{\mathbb{K}/\Bbbk}(\alpha) &= r(\alpha_1 + \cdots + \alpha_d). \end{aligned}$$

We know that α is a root of the polynomial $p(x) \in \Bbbk[x]$, for any $\sigma \in G = \mathrm{Gal}(\mathbb{K}/\Bbbk)$, σ fixes p, so $\sigma(\alpha) = \alpha_i$ for some $1 \leq i \leq d$. $\mathbb{K}/\Bbbk$ is a Galois extension, so there exists $\sigma_i \in G$ such that $\sigma_i(\alpha) = \alpha_i$ for all $1 \leq i \leq d$. Let $G_\alpha = \mathrm{Gal}(\mathbb{K}/\Bbbk(\alpha))$. We have proved in Exercise 11.6.2 that $\bigcup_{i=1}^d (\sigma_i G_\alpha)$ is a coset partition of G with respect to the subgroup G_α. Each coset has r elements and for any $\tau \in \sigma_i G_\alpha$, $\tau(\alpha) = \alpha_i$. Therefore, we have

$$\begin{aligned} N_{\mathbb{K}/\Bbbk}(\alpha) &= \prod_{\sigma \in G} \sigma(\alpha) = (\prod_{i=1}^d \sigma_i(\alpha))^r = (\alpha_1 \cdots \alpha_d)^r, \\ T_{\mathbb{K}/\Bbbk}(\alpha) &= \sum_{\sigma \in G} \sigma(\alpha) = r(\sum_{i=1}^d \sigma_i(\alpha)) = r(\alpha + \cdots + \alpha_d). \end{aligned}$$

Problem 12.4.11
Let $a, b \in \mathbb{Q}$.

(a) $a^2 + b^2 = 1$ is equivalent to $N_{\mathbb{Q}(i)/\mathbb{Q}}(a + ib) = 1$.

(b) Use Hilbert's Theorem 90 to prove that the rational solutions of $a^2 + b^2 = 1$ are of the form $a = (s^2 - t^2)/(s^2 + t^2)$ and $b = 2st/(s^2 + t^2)$ for $s, t \in \mathbb{Q}$.

Solution:

(a) We have proved in Exercise 12.4.9 that $N_{\mathbb{Q}(i)/\mathbb{Q}}(a + ib) = \det A_{a+ib}$ where A_{a+ib} is the matrix given by the multiplication $x \mapsto (a+ib)x$ for all $x \in \mathbb{Q}(i)$. Choose $\{1, i\}$ as a $\mathbb{Q}$-basis for $\mathbb{Q}(i)$ and the matrix A_{a+ib} can be written as

$$A_{a+ib} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

By direct calculation, we know that

$$N_{\mathbb{Q}(i)/\mathbb{Q}}(a + ib) = \det A_{a+ib} = a^2 + b^2.$$

Therefore, $a^2 + b^2 = 1$ is equivalent to $N_{\mathbb{Q}(i)/\mathbb{Q}}(a + ib) = 1$.

(b) From (a), we know that $a^2+b^2 = 1$ has rational solutions if and only if $N_{\mathbb{Q}(i)/\mathbb{Q}}(a+ib) = 1$. We know that $\mathbb{Q}(i)/\mathbb{Q}$ is a quadratic extension so the Galois group $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = C^2$ generated by sending i to $-i$. Choose $\{1, i\}$ as a $\mathbb{Q}$-basis for $\mathbb{Q}(i)$. By Hilbert's Theorem 90, there exists $s + it \in \mathbb{Q}(i)$ for some $t, s \in \mathbb{Q}$ and $s^2 + t^2 \neq 0$ such that

$$\frac{s + it}{s - it} = a + ib.$$

This is equivalent to

$$\frac{(s^2 - t^2 + i(2st))}{s^2 + t^2} = a + ib.$$

By comparing coefficients we know that a, b must have the form

$$a = \frac{s^2 - t^2}{s^2 + t^2},$$
$$b = \frac{2st}{s^2 + t^2}.$$

Problem 13.2.9
True or false? Let $\mathbb{K}/\mathbb{F}_q$ be a finite extension, and $\mathbb{L}$, $\mathbb{M}$ be two intermediate subfields. Then either $\mathbb{L} \subseteq \mathbb{M}$ or $\mathbb{M} \subseteq \mathbb{L}$.

Solution: This is true. Suppose $q = p^d$ for some prime p. Then the field extension $\mathbb{K}/\mathbb{F}_q$ must be $\mathbb{K} \cong \mathbb{F}_{p^n}$ for some n satisfying $d|n$ by Corollary 13.2.8. We know the Galois group $\mathrm{Gal}(\mathbb{K}/\mathbb{F}_q)$ is isomorphic to the cyclic group $C_{n/d}$. By Galois correspondence, $\mathbb{M}^*$ and $\mathbb{L}^*$ are subgroups of $C_{n/d}$. We know in cyclic groups, either $\mathbb{M}^* \subseteq \mathbb{L}^*$ or $\mathbb{L}^* \subseteq \mathbb{M}^*$. This implies $\mathbb{L} \subseteq \mathbb{M}$ or $\mathbb{L} \subseteq \mathbb{M}$.

Problem 13.2.12
Let p be a prime. Then there are exactly $(q^p - q)/p$ monic irreducible polynomials of degree p in $\mathbb{F}_q[x]$ (q is not necessarily a power of p).

Solution: Let $\mathbb{K}$ be a degree p extension of $\mathbb{F}_q$. Then $\mathbb{K}$ is a p dimensional $\mathbb{F}_q$-vector space, thus having q^p elements. By Theorem 13.2.3, $\mathbb{K}$ is the splitting field of the polynomial $x^{q^p} - x$. The field $\mathbb{K}$ has exactly q^p elements, so $x^{q^p} - x$ has q^p different roots in $\mathbb{K}$. Let $f \in \mathbb{F}_q[x]$ be a degree p irreducible polynomial. If α is a root of f, then $\mathbb{F}_q(\alpha)/\mathbb{F}_q$ is a degree p extension and thus, $\mathbb{F}_q(\alpha) \cong \mathbb{K}$ as a finite field extension. This means α is also a root of the polynomial $x^{q^p} - x$. Since every finite field is separable, every irreducible polynomial f contributes p different roots for the polynomial $x^{q^p} - x$. Note that $[\mathbb{K} : \mathbb{F}_q] = p$ is a prime number, only 1 and p divides $[\mathbb{K} : \mathbb{F}_q]$, so the roots of $x^{q^p} - x$ either coming from a degree p irreducible polynomial or coming from a degree 1 irreducible polynomial. We have q elements in $\mathbb{F}_q$, which counts as q irreducible degree 1 polynomial. So the number of degree p polynomial over $\mathbb{F}_q$ is equal to $\frac{q^p - q}{p}$.

Problem 13.2.13
What is $\sum_A A^{100}$, where the sum is over all 17×17 matrices A over $\mathbb{F}_{17}$?

Solution: We know that $\mathbb{F}_{17}^{\times}$ is a multiplicative group generated by a where $a^{16} = 1$. We first prove a claim.
<u>Claim:</u> The sum over all elements $x \in \mathbb{F}_{17}$ is $\sum_{x \in \mathbb{F}_{17}} x^{100} = 0$.
<u>Proof:</u> Write $S = \sum_{x \in \mathbb{F}_{17}} x^{100}$. Consider $a^{100}S$. Note that a acting by multiplication on the field

$$\mathbb{F}_{17} = \left\{0, 1, a, a^2, \ldots, a^{16}\right\}$$

is just a permutation of these elements. So we have

$$a^{100}S = a^{100} \sum_{x \in \mathbb{F}_{17}} x^{100} = \sum_{x \in \mathbb{F}_{17}} (ax)^{100} = \sum_{x \in \mathbb{F}_{17}} x^{100} = S.$$

This implies $(a^{100} - 1)S = 0$ in the field $\mathbb{F}_{17}$. Since $16 \nmid 100$, $a^{100} - 1 \neq 0$. This implies $S = 0$. ■

Now consider a^{100} acts on a matrix $A \in M_{17}(\mathbb{F}_{17})$ by multiplication on each entry. We have

$$a^{100} \sum_A A^{100} = \sum_A (aA)^{100}.$$

We claim the following map

$$\begin{aligned} m_a : M_{17}(\mathbb{F}_{17}) &\to M_{17}(\mathbb{F}_{17}), \\ A &\mapsto aA \end{aligned}$$

is a bijection. Indeed, since a is multiplicatively invertible in $\mathbb{F}_{17}$, multiplying by $\frac{1}{a} = a^{15}$ is the inverse map. So m_a is both injective and surjective. By the same argument as in the claim on each entry, we have $\sum_A A^{100} = 0$.