

HOMEWORK 9

Due date: Tuesday of Week 10

Exercises: M.2, M.4, M.5, M.7, page 475-476; Exercises: 3.1, 3.2, 3.3, page 506 of Artin's book. For M.5, just prove the assertion, no matter what you use. For M.7, one can show that the reduction map $\mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective for any positive integer N . For Exercise 3.1, page 506, use induction on n .

Recall the following basic terminologies. Let F be a field and $f \in F[x]$. Then f is called separable if f has no multiple roots (or it has no repeated roots) over any field extension K/F . An equivalent condition is $\gcd(f, f') = 1$. The field F is called perfect if any irreducible $f \in F[x]$ is separable.

Problem 1. Let F be a field of characteristic $p > 0$.

- (1) Given $a \in F$. Show that $x^p - a \in F[x]$ is either irreducible or a power $(x - \beta)^p$ for some $\beta \in F$.
- (2) Define $F^p := \{x^p : x \in F\} \subset F$. Show that F is perfect iff $F = F^p$.
- (3) Show that the finite field \mathbb{F}_q is perfect, where $q = p^r$ for some prime integer p .

Hint: (1) is basically proved in class. The direction \implies of (2) follows from (1). For the direction \impliedby of (2), prove it by contradiction. It is related to Exercise 7.10, page 474 of Artin's book.

Problem 2. Let F be a perfect field and $f \in F[x]$. Show that the following are equivalent:

- (1) f is separable, i.e., f has no multiple roots over any field extension K/F ;
- (2) $\gcd(f, f') = 1$;
- (3) f is a product of distinct irreducible polynomials, namely $f = p_1 p_2 \dots p_k$, with $p_i \in F[x]$ irreducible and distinct.

The equivalence of (1) and (2) is Proposition 15.6.7, page 458, Artin's book. Please repeat it here. This is a generalization of the Lemma in page 266 of Hoffman-Kunze. Actually the equivalence of (2) and (3) can be proved in the same way as the proof of the Lemma in page 266 of Hoffman-Kunze.

Recall that a field extension K/F is called separable if for any $\alpha \in K$, its minimal polynomial is separable.

Problem 3. Let $\eta : F \rightarrow F'$ be an isomorphism of fields and let K/F be a separable finite extension of degree n . Let Ω be an algebraically closed field which contains F, F', K . Consider the set

$$I(K, \eta, F, F') = \{\sigma : K \rightarrow \Omega : \sigma(a) = \eta(a), \forall a \in F\}.$$

Show that $|I(K, \eta, F, F')| = n$.

An element $\sigma \in I(K, \eta, F, F')$ is called an extension of η to K . The following is an outline of the proof. Fill some details.

Proof of Problem 3. Take $\alpha \in K$ but $\alpha \notin F$. Consider $I(F(\alpha), \eta, F, F')$. If $\tau \in I(F(\alpha), \eta, F, F')$, then $\tau : F(\alpha) \rightarrow \Omega$ is uniquely determined by the value $\tau(\alpha)$. Let $\mu_\alpha \in F[x]$ be the minimal polynomial of α . By assumption μ_α is separable. Moreover, $\tau(\alpha)$ is a root of $\eta(\mu_\alpha) \in F'[x]$. Now $\eta(\mu_\alpha)$ is also separable (check it) and it has m distinct roots in Ω with $m = [F(\alpha) : F] > 1$. Now $\tau(\alpha)$ is uniquely determined by such a root and thus there are m elements in $I(F(\alpha), \eta, F, F')$, say $\{\tau_1, \dots, \tau_m\}$. If $F(\alpha) = K$, we are done. If not, by induction, there are r elements in each $I(K, \tau_i, F(\alpha), \tau_i(F(\alpha)))$, say $\{\sigma_{i1}, \dots, \sigma_{ir}\}$, with $r = [K : F(\alpha)] < n$. Now check $I(K, \eta, F, F') = \{\sigma_{ij}, 1 \leq i \leq m, 1 \leq j \leq r\}$. Thus $|I(K, \eta, F, F')| = rm = n$. \square

Problem 4. Assume that K/F be a separable field extension of degree n . Let Ω be an algebraically closed field such that $F \subset K \subset \Omega$ (such a field always exists). Show that there are n distinct F -embeddings $\sigma : K \rightarrow \Omega$ (an F -embedding is a field homomorphism such that $\sigma(a) = a, \forall a \in F$). Moreover, for any $\alpha \in K$, and any F -embedding $\tau : F(\alpha) \rightarrow \Omega$, show that $|I(K, \tau, F(\alpha), \tau(F(\alpha)))| = [K : F(\alpha)]$.

This is a corollary of the last problem. The statement is an important characteristic property of separable extension. If K/F is also normal, then an F -embedding $\sigma : K \rightarrow \Omega$ is actually an F -isomorphism $K \rightarrow K$, and thus an element in $\text{Gal}(K/F)$. In this case, the assertion is proved in class.

Problem 5. Construct a splitting field of the polynomial $f = x^5 - 2 \in \mathbb{Q}[x]$ over \mathbb{Q} . Find its dimension over \mathbb{Q} .

1. MORE ON TRACES AND NORMS

Problem 6. Let K/F be a finite field extension and let E be any intermediate field (namely, $F \subset E \subset K$). Given $\alpha \in K$, we can consider the tower $F \subset E \subset E(\alpha) \subset K$.

(1) Show that

$$\text{Tr}_{K/E}(\alpha) = \text{Tr}_{E(\alpha)/E}(\text{Tr}_{K/E(\alpha)}(\alpha)), \text{ and } \text{Nm}_{K/E}(\alpha) = \text{Nm}_{E(\alpha)/E}(\text{Nm}_{K/E(\alpha)}(\alpha))$$

(2) Show that

$$\text{Tr}_{K/F}(\alpha) = \text{Tr}_{E(\alpha)/F}(\text{Tr}_{K/E(\alpha)}(\alpha)), \text{ and } \text{Nm}_{K/F}(\alpha) = \text{Nm}_{E(\alpha)/F}(\text{Nm}_{K/E(\alpha)}(\alpha))$$

(3) Show that

$$\text{Tr}_{E(\alpha)/F}(\alpha) = \text{Tr}_{E/F}(\text{Tr}_{E(\alpha)/E}(\alpha)), \text{ and } \text{Nm}_{E(\alpha)/F}(\alpha) = \text{Nm}_{E/F}(\text{Nm}_{E(\alpha)/E}(\alpha)).$$

(4) Show that

$$\text{Tr}_{K/F}(\alpha) = \text{Tr}_{E/F}(\text{Tr}_{K/E}(\alpha)), \text{ and } \text{Nm}_{K/F}(\alpha) = \text{Nm}_{E/F}(\text{Nm}_{K/E}(\alpha)).$$

(4) follows from (1) (2) and (3) directly. (1) is actually proved in last HW. See Problem 5 (5), HW8. Proof of (2) should be easy. Proof of (3) is complicate but it is standard linear algebra. This problem is related to a problem of HW11, 2023. Here is an explanation. View K as a vector space over E and consider the linear operator $T_{\alpha, E} : K \cong E^m \rightarrow K \cong E^m$, which defines an matrix in $A = \text{Mat}_{m \times m}(E)$, where $m = [K : E]$. We can also view E as a vector space over F of dimension n with $n = [E : F]$ and thus $E^m \cong F^{mn}$. The same map defines a matrix in $B \in \text{Mat}_{(mn) \times (mn)}(F)$. What is the relation between $\det(A) \in E$ and $\det(B) \in F$? The answer given by (4) is $\det(B) = \text{Nm}_{E/F}(\det(A))$. This is roughly explained in HW11, 2023, and was proved there when $E/F = \mathbb{C}/\mathbb{R}$. (4) can be proved directly and $\det(B) = \text{Nm}_{E/F}(\det(A))$ is true more generally, which means that the matrix A need not to come from a field extension K/E . Check HW11, 2023 and the reference given there.

Problem 7. Let K/F be an extension of fields degree n . Let $\alpha \in K$ and $f = \mu_\alpha$ be the minimal polynomial of α . Let $\alpha_1, \dots, \alpha_m$ be all the roots of f in some extension of F . Here $m = \deg(f)$ and we can choose $\alpha_1 = \alpha$. Show that

$$\text{Tr}_{K/F}(\alpha) = r(\alpha_1 + \dots + \alpha_m),$$

and

$$\text{Nm}_{K/F}(\alpha) = (\alpha_1 \cdots \alpha_m)^r,$$

where $r = [K : F(\alpha)] = n/m$.

Problem 8. Let K/F be a separable field extension of degree n . Let Ω be an algebraically closed field such that $F \subset K \subset \Omega$ (such a field always exists). We know that there are n distinct F -embeddings $\sigma : K \rightarrow \Omega$ by Problem 3 (an F -embedding is a field homomorphism such that $\sigma(a) = a, \forall a \in F$). Denote all such F -embeddings by $\{\sigma_1, \dots, \sigma_n\}$. Show that

$$\text{Tr}_{K/F}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha), \text{ and } \text{Nm}_{K/F}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha).$$

Hint: This is a corollary of Problem 4 and Problem 7.

Here is one example. Let $F = \mathbb{Q}$ and $K = \mathbb{Q}(\alpha)$ with $\alpha = \sqrt[3]{2}$. Take $\Omega = \mathbb{C}$. Then all the \mathbb{Q} -embeddings $K \rightarrow \mathbb{C}$ are $\{\sigma_1, \sigma_2, \sigma_3\}$, where $\sigma_1(\alpha) = \alpha$, $\sigma_2(\alpha) = \omega\alpha$ and $\sigma_3(\alpha) = \omega^2\alpha$ with $\omega = e^{2\pi\sqrt{-1}/3}$. Note that α is a root of $x^3 - 2 = 0$ and thus $\sigma(\alpha)$ must be also a root of $x^3 - 2 = 0$. When K/F is Galois, it is easy to show that $\{\sigma_1, \dots, \sigma_n\} = \text{Gal}(K/F)$ and thus

$$\text{Tr}_{K/F}(\alpha) = \sum_{\sigma \in \text{Gal}(K/F)} \sigma(\alpha), \text{ and } \text{Nm}_{K/F}(\alpha) = \prod_{\sigma \in \text{Gal}(K/F)} \sigma(\alpha).$$

The assertion of Problem 8 is false if F/K is not separable. See the next problem.

Problem 9. Let $F = \mathbb{F}_2(x)$ (the fractional field of the polynomial ring $\mathbb{F}_2[x]$) and let $K = F(\sqrt{x}) = F[y]/(y - x^2)$. Show that $\text{Tr}_{K/F}(\alpha) = 0$ for any $\alpha \in K$. Moreover, check the assertion of the last problem is false in this example.

If K/F is finite separable extension, then one can show that $\text{Tr}_{K/F}$ is not a zero map. If characteristic of F is zero, then this is of course trivial, because $\text{Tr}_{K/F}(1) = [K : F] \neq 0$. If characteristic of F is $p > 0$, it need some work. We might prove this in future HW.