Math 121 Homework 6 Solutions

Problem 14.2 # 17. Let $K/F$ be any finite extension and let $\alpha \in K$. Let $L$ be a Galois extension of $F$ containing $K$ and let $H \leq \text{Gal}(L/F)$ be the subgroup corresponding to $K$. Define the norm of $\alpha$ from $K$ to $F$ to be

$$N_{K/F}(\alpha) = \prod_{\sigma} \sigma(\alpha),$$

where the product is taken over all embeddings of $K$ into an algebraic closure of $F$ (so over a set of coset representatives for $H$ in $\text{Gal}(L/F)$ by the Fundamental Theorem of Galois Theory.) In particular if $K/F$ is Galois this is $\prod_{\sigma \in \text{Gal}(K/F)} \sigma(\alpha)$.

(a) Prove that $N_{K/F}(\alpha) \in F$.

(b) Prove that $N_{K/F}(\alpha \beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$, so the norm is a multiplicative map from $K$ to $F$.

(c) Let $K = F\left(\sqrt{D}\right)$ be a quadratic extension of $K$. Show that

$$N_{K/F}\left(a + b\sqrt{D}\right) = a^2 - Db^2.$$

(d) Let $m_{\alpha}(x) = x^d + a_{d-1}x^{d-1} + \ldots + a_1x + a_0$ be the minimal polynomial of $\alpha \in K$ over $F$. Let $n = [K : F]$. Prove that $d|n$, that there are $d$ distinct Galois conjugates of $\alpha$ which are all repeated $n/d$ times in the product above, and conclude that $N_{K/F}(\alpha) = (-1)^n a_0^{n/d}$.

Solution. We review some points that are made in the proof of Theorem 14 (The Fundamental Theorem of Galois Theory), page 575-6.

We may take the algebraic closure $\overline{F}$ of $F$ to contain $L$. We will denote $G = \text{Gal}(L/K)$.

Lemma 1. Let $G = \text{Gal}(L/F)$ and $H = \text{Gal}(L/K) \subseteq G$. Then every embedding $\sigma : K \rightarrow \overline{F}$ extends to an automorphism $\sigma_1 \in G$, and $\sigma_1, \sigma_2 \in G$
have the same restriction to $K$ if and only if they represent the same coset $\sigma_1 H = \sigma_2 H$. Therefore the distinct embeddings of $K$ into $\overline{F}$ over $F$ are in bijection with the cosets $\sigma H$.

Proof. Since $L$ is a splitting field, every embedding $\sigma : K \rightarrow \overline{F}$ has image in $L$, and extends to an automorphism of $L$. If $\sigma_1$ and $\sigma_2 \in \text{Gal}(L/K)$ are two such extensions, then they are the same if $\sigma_1(x) = \sigma_2(x)$ for all $x \in K$, in other words, $\sigma_1^{-1}\sigma_2(x) = x$ which means $\sigma_1^{-1}\sigma \in \text{Gal}(L/K) = H$. This is equivalent to $\sigma_1 H = \sigma_2 H$. \qed

So we can write

$$N_{K/F}(\alpha) = \sum_{\text{cosets } \sigma H \atop \sigma \in G} \sigma(\alpha).$$

(1)

Now let us show $N_{K/F}(\alpha) \in F$. Since $F$ is the fixed field of $G$, it is sufficient to show that $\tau N_{K/F}(\alpha) = N_{K/F}(\alpha)$ for $\tau \in G$. This is because $\sigma H \rightarrow \tau \sigma H$ is a permutation of the cosets and so

$$N_{K/F}(\alpha) = \sum_{\text{cosets } \sigma H \atop \sigma \in G} \sigma(\alpha) = \sum_{\text{cosets } \tau \sigma H \atop \sigma \in G} \tau \sigma(\alpha) = \tau \left( \sum_{\text{cosets } \sigma H \atop \sigma \in G} \sigma(\alpha) \right) = \tau N_{K/F}(\alpha).$$

This proves (a).

As for (b), $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ and taking the product over all embeddings $\sigma$ of $K$ into $L$ over $F$ gives $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$.

For (c), the assumption that $F \left( \sqrt{D} \right)$ is a quadratic extension of $K$ implies that the polynomial $x^2 - D$ is irreducible over $F$. Its roots are $\sqrt{D}$ and $-\sqrt{D}$, so $N_{K/F} \left( \alpha + b\sqrt{D} \right) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - D\bar{b}^2$.

Before we prove (d), we will prove another important property of the norm.

**Proposition 2.** Let $E \supset K \supset F$ and let $\alpha \in E$. Then $N_{E/F}(\alpha) = N_{K/F}(N_{E/K}(\alpha))$.

This property is sometimes called the *transitivity of the norm map*.
Proof. We may choose the Galois extension $L$ of $F$ in the definition of the norm so that it contains both $K$ and $E$. Let $H = \text{Gal}(L/K)$ as before, and let $M = \text{Gal}(L/E)$ so $M \subseteq H$.

Now we can choose coset representatives for $M$ in $G$ as follows. First, let $\sigma_1, \cdots, \sigma_k$ be left coset representatives for $H = \text{Gal}(L/K)$ in $G = \text{Gal}(L/F)$. This means

$$G = \bigcup_i \sigma_i H \quad \text{(disjoint)}.$$ 

Similarly, let $\tau_1, \cdots, \tau_l$ be left coset representatives for $M$ in $H$, so

$$H = \bigcup_j \tau_j M \quad \text{(disjoint)}.$$ 

Then

$$G = \bigcup_i \sigma_i H = \bigcup_{i,j} \sigma_i \tau_j M,$$

so the $\sigma_i \tau_j$ are a set of coset representatives for $M$ in $G$. This means that

$$N_{E/F}(\alpha) = \sum_{i,j} \sigma_i \tau_j(\alpha) = \sum_i \sigma_i \left( \sum_j \tau_j \alpha \right) = \sum_i \sigma_i (N_{E/K}(\alpha)) = N_{K/F}(N_{E/K}(\alpha)).$$

Now let us prove (d). We have inclusions $K \supseteq F(\alpha) \supseteq F$. Let $[F(\alpha) : F] = d$ so $[K : F(\alpha)] = n/d$. By the transitivity of the norm, $N_{K/F}(\alpha) = N_{F(\alpha)/F} N_{K/F(\alpha)}(\alpha)$. Since $\alpha \in F(\alpha)$, $\tau(\alpha) = \alpha$ for every embedding of $K$ into $L$ over $F(\alpha)$, and there are $n/d$ such embeddings, so

$$N_{K/F(\alpha)}(\alpha) = \prod_{\tau} \tau(\alpha) = \alpha^{n/d}.$$ 

Now let us compute $N_{F(\alpha)/F}(\alpha)$. This is the product of the conjugates $\sigma(\alpha)$ of $\alpha$. These are the distinct roots of the minimal polynomial

$$\prod_{i=1}^d (x - \sigma_i \alpha).$$
(The roots of this polynomial are all distinct since $L/F$ is Galois and therefore separable, and so any intermediate extension such as $F(\alpha)/F$ is separable.) The constant term $a_0$ of this polynomial is then $(-1)^d \prod \sigma_i(\alpha) = (-1)^d N_{F(\alpha)/F}(\alpha)$. Therefore

$$N_{K/F}(\alpha) = N_{F(\alpha)/F}N_{K/F(\alpha)}(\alpha) = N_{F(\alpha)/F}(\alpha^{n/d}) = (N_{F(\alpha)/F}(\alpha))^{n/d} = ((-1)^d a_0)^{n/d} = (-1)^n a_0^{n/d}.$$ 

**Problem 14.2 #18.** With notation as in the previous problem, define the trace of $\alpha$ from $K$ to $F$ to be

$$\text{Tr}_{K/F}(\alpha) = \sum_{\sigma} \sigma(\alpha),$$

a sum of Galois conjugates of $\alpha$.

(a) Prove that $\text{Tr}_{K/F}(\alpha) \in F$.

(b) Prove that $\text{Tr}_{K/F}(\alpha + \beta) = \text{Tr}_{K/F}(\alpha) + \text{Tr}_{K/F}(\beta)$, so that the trace is an additive map from $K$ to $F$.

(c) Let $K = F(\sqrt{D})$ be a quadratic extension of $K$. Show that $\text{Tr}_{K/F}(a + b\sqrt{D}) = 2a$.

(d) Let $m_{\alpha}(x)$ be as in the previous problem. Prove that $\text{Tr}_{K/F}(\alpha) = -\frac{n}{d} a_{d-1}$.

**Solution:** This is so similar to the previous problem that we won’t write out solutions to (a) and (b). For (c), as in the previous problem the conjugates of $a + b\sqrt{D}$ over $F$ are $a + b\sqrt{D}$ and $a - b\sqrt{D}$, so the trace is the sum $2a$ of these. For (d), this is also similar to the previous problem. We may use the transitivity property of the trace:

**Proposition 3.** Let $E \supset K \supset F$ and let $\alpha \in E$. Then $\text{Tr}_{E/F}(\alpha) = \text{Tr}_{K/F}(\text{Tr}_{E/K}(\alpha))$.

**Problem 14.2 #21.** Use the linear independence of characters to show that for any Galois extension $K$ of $F$ there is an element $\alpha \in K$ with $\text{Tr}_{K/F}(\alpha) \neq 0$.

**Solution:** The linear independence of characters is Theorem 7 on page 569. It is due to Artin. Since $K/F$ is Galois, then

$$\text{Tr}_{K/F}(\alpha) = \sum_{\chi \in \text{Gal}(K/F)} \chi(\alpha).$$

If this is always zero, then $\sum \chi = 0$, contradicting Theorem 7 with all $a_i = 1$. 

4
**Problem 14.2 #22.** Suppose $K/F$ is a Galois extension of $F$ and let $\sigma$ be an element of $\text{Gal}(K/F)$.

(a) Suppose that $\alpha \in K$ is of the form $\alpha = \beta \sigma \beta$ for some nonzero $\beta \in K$. Prove that $N_{K/F}(\alpha) = 1$.

(b) Suppose that $\alpha \in K$ is of the form $\alpha = \beta - \sigma \beta$ for some $\beta \in K$. Prove that $\text{Tr}_{K/F}(\alpha) = 0$.

This problem sets up Hilbert’s Theorem 90 (Exercise 23) which we will be discussing later.

**Solution:** Since $K/F$ is Galois,

$$N(\beta) = \prod_{\tau \in \text{Gal}(K/F)} \tau(\beta), \quad N(\sigma \beta) = \prod_{\tau \in \text{Gal}(K/F)} \tau \sigma(\beta),$$

But $\tau \mapsto \tau \sigma$ just permutes the elements of $\text{Gal}(K/F)$. Therefore $N(\beta) = N(\sigma(\beta))$. Thus $N(\beta/\sigma \beta) = N(\beta)/N(\sigma \beta) = 1$. Part (b) is similar.

**Problem 14.3 #9.** Let $q = p^m$ be a power of the prime $p$ and let $\mathbb{F}_q = \mathbb{F}_{p^m}$ be the finite field with $q$ elements. Let $\sigma_q = \sigma_p^m$ be the $m$-th power of the Frobenius automorphism $\sigma_p$, called the $q$-Frobenius automorphism.

(a) Prove that $\sigma_q$ fixes $\mathbb{F}_q$.

(b) Prove that every finite extension of $\mathbb{F}_q$ of degree $n$ is the splitting field of $x^{q^n} - x$ over $\mathbb{F}_q$, and hence there is a unique such extension.

(c) Prove that every finite extension of $\mathbb{F}_q$ of degree $n$ is cyclic with $\sigma_q$ as a generator.

(d) Prove that the subfields of the unique extension of $\mathbb{F}_q$ of degree $n$ are in bijection with the divisors $d$ of $n$.

**Solution.** This problem is very similar to Proposition 15 on page 586. We could argue some points alternatively by making more use of Proposition 15.

(a) We may interpret $\sigma_q$ as an automorphism of any field containing $\mathbb{F}_p$, in particular of $\mathbb{F}_q$. But as an automorphism of $\mathbb{F}_q$, it is trivial, and this is the content of (a). To see this, we must show that $\sigma_q(a) = a$ if $a \in \mathbb{F}_q$, that is, $a^q = a$. If $a = 0$ this is obvious, so assume that $a \in \mathbb{F}_q^\times$. This is a finite group of order $q - 1$, so $a^{q - 1} = 1$. Multiplying this equation by $a$ gives $a^q = a$.

(b) If $[E : \mathbb{F}_q] = n$, then $E$ is a vector space of dimension $n$ over $\mathbb{F}_q$, so $E$ has cardinality $q^n$. Now if $a \in E$, then we claim $a^{q^n} = a$. We may prove this the same way as (a): if $x = 0$ this is clear, and if $a \neq 0$, then $a$ lies in a group $E^\times$ of order $q^n - 1$, so $a^{q^n - 1} = 1$, so $a^{q^n} = a$. Now the polynomial
\( f(x) = x^{q^n} - x \) is separable, since \( f'(x) = -1 \), so \( f \) and \( f' \) are coprime. Thus its roots are distinct, but we have shown that the \( q^n \) elements of \( E \) are roots, so the elements of \( E \) are precisely the roots of this polynomial in an algebraic closure of \( E \). It is now clear that \( E \) is the splitting field of \( f \).

(c) With \( F = \mathbb{F}_q \) and \( E = \mathbb{F}_{q^n} \), the field \( E \) is the splitting field of a separable polynomial, so it is Galois over \( E \). The group \( G = \text{Gal}(E/F) \) has order \( n = [E : F] \), and \( \sigma_q \) is an element. To show that it is cyclic with generator \( \sigma_q \) sufficient to show that if \( m \) is a divisor of \( n = |G| \) and \( \sigma_q^m = 1_E \) then \( m = n \). Indeed, for all \( a \in E \), we have \( a = \sigma_q^m(a) = a^{q^m} \), so the polynomial \( x^{q^n} - x \) has \( q^n \) roots, namely all elements of \( E \). Because a polynomial of degree \( q^m \) cannot have more than \( q^m \) roots, we must have \( m = n \).

(d) This now follows from the fundamental theorem of Galois theory, since a cyclic group of order \( n \) has one subgroup for each divisor of \( n \).

Problem 14.3 #10. Prove that \( n \) divides \( \varphi(p^n - 1) \). [Hint: observe that \( \varphi(p^n - 1) \) is the order of the group of automorphisms of a cyclic group of order \( p^n - 1 \).]

Solution. By Proposition 16 on page 135 of Dummit and Foote, the group of automorphisms of the cyclic group \( \mathbb{Z}_m \) of order \( m \) is \( (\mathbb{Z}/m\mathbb{Z})^\times \), which has order \( \phi(m) \). We apply this with \( m = p^n - 1 \). The group \( \mathbb{F}_{p^n}^\times \) is cyclic of order \( p^n - 1 \) so \( \text{Aut}(\mathbb{F}_{p^n}^\times) \) has order \( \phi(p^n - 1) \). Now we may exhibit an automorphism of order exactly \( n \), namely the Frobenius map \( x \mapsto x^p \). By Lagrange’s theorem, every element of \( \text{Aut}(\mathbb{F}_{p^n}^\times) \) must have order dividing \( |\text{Aut}(\mathbb{F}_{p^n}^\times)| \) and so \( n | p^n - 1 \).

Problem 14.5 #3. Determine the quadratic equation satisfied by the period \( \alpha = \zeta_5 + \zeta_5^{-1} \) of the fifth root of unity \( \zeta_5 \). Determine the quadratic equation satisfied by \( \zeta_5 \) over \( \mathbb{Q}(\alpha) \) and use this to explicitly solve for the fifth root of unity.

Solution. Let \( \sigma \in \text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \). Then \( \sigma(\zeta_5) = \zeta_5^a \) where \( a \) can be 1, 2, -1 or -2. So \( \sigma(\zeta_5) = \zeta_5^a + \zeta_5^{-a} \cdot \frac{\alpha + \sqrt{\alpha^2 - 4}}{2} \). This means that the conjugates of \( \alpha \) are \( \alpha = \zeta_5 + \zeta_5^{-1} \) and \( \beta = \zeta_5^2 + \zeta_5^{-2} \). Now

\[
1 + \alpha + \beta = 1 + \zeta_5 + \zeta_5^{-1} + \zeta_5^2 + \zeta_5^{-2} = 0.
\]

Also

\[
\alpha \beta = (\zeta_5 + \zeta_5^{-1})(\zeta_5^2 + \zeta_5^{-2}) = \zeta_5^3 + \zeta_5^{-1} + \zeta_5 + \zeta_5^{-3} = -1.
\]
Since $\alpha + b = \alpha \beta = -1$ we have
\[(x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha \beta = x^2 + x - 1.\]
The $f(x) = x^2 + x - 1$ is the quadratic equation satisfied by $\alpha, \beta$ and so $\alpha, \beta$ are
\[-\frac{1 \pm \sqrt{5}}{2}.
\]
With $\zeta_5 = e^{2\pi i/5}$ we have $\alpha = 2 \cos \left(\frac{2\pi}{5}\right) > 0$ since $0 < \frac{2\pi}{5} < \frac{\pi}{2}$, while $\beta = 2 \cos \left(\frac{4\pi}{5}\right) < 0$. So
\[\alpha = \frac{\sqrt{5} - 1}{2}, \quad \beta = -\frac{\sqrt{5} + 1}{2}.
\]
Now we are asked to find the quadratic equation satisfied by $\zeta = \zeta_5$ over $\mathbb{Q}(\alpha)$. Since $\alpha$ is real, complex conjugation $\sigma_{-1} \in \text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}(\alpha))$. Thus the conjugates of $\zeta$ over $\mathbb{Q}(\alpha)$ are $\zeta$ and $\zeta^{-1}$, and the irreducible polynomial they satisfy is
\[(x - \zeta)(x - \zeta^{-1}) = x^2 - \alpha x + 1.\]
Using the quadratic equation again,
\[\zeta = \frac{\alpha \pm \sqrt{\alpha^2 - 4}}{2}.
\]
Here $\alpha^2 - 4 < 0$ so if we interpret the square root as $(\sqrt{4 - \alpha^2})i$ then we want the positive sign because $\zeta$ has positive imaginary part $\sin \left(\frac{2\pi}{5}\right)$. Thus
\[\zeta = \frac{\alpha + \sqrt{\alpha^2 - 4}}{2}.
\]
**Problem 14.5 #4.** Let $\sigma_a \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ denote the automorphism of the cyclotomic field of $n$-th roots of unity such that $\sigma_a(\zeta_n) = \zeta_n^a$. Show that $\sigma_a(\zeta) = \zeta^a$ for every $n$-th root of unity $\zeta$.

**Solution.** For some $m$ we have $\zeta = \zeta_n^m$. Therefore $\sigma_a(\zeta) = \sigma_a(\zeta_n)^m = \zeta_n^{am} = (\zeta_n^m)^a = \zeta^a$.  

7