Math 121 Homework 6 Solutions

- Section 14.2 # 17a, 17b, 17c, 22a
- Section 14.3 # 8, 9a, 9b

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 $H \leqslant \mathrm{Gal}(L/F)$ be the subgroup corresponding to K. Define the *norm* of α 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 $\mathrm{Gal}(L/F)$ by the Fundamental Theorem of Galois Theory.) In particular if K/F is Galois this is $\prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha)$.

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

(b) Prove that $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(b)$, 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

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

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 $G = \mathrm{Gal}(L/K)$.

Lemma 1. *Let $G = \mathrm{Gal}(L/F)$ and $H = \mathrm{Gal}(L/K) \subseteq G$. Then every embedding $\sigma : K \longrightarrow \overline{F}$ 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 σH.*

Proof. Since L is a splitting field, every embedding $\sigma : K \longrightarrow \overline{F}$ has image in L, and extends to an automorphism of L. If σ_1 and $\sigma_2 \in \mathrm{Gal}(L/K)$ 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 $\sigma_1^{-1}\sigma \in \mathrm{Gal}(L/K) = H$. This is equivalent to $\sigma_1 H = \sigma_2 H$. $\square$

So we can write

$$N_{K/F}(\alpha) = \sum_{\substack{\text{cosets } \sigma H \\ \sigma \in G}} \sigma(\alpha). \tag{1}$$

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 $\sigma H \to \tau\sigma H$ is a permutation of the cosets and so

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

This proves (a).

As for (b), $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ and taking the product over all embeddings σ 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 $N_{K/F}\left(\alpha + b\sqrt{D}\right) = \left(a + b\sqrt{D}\right)\left(a - b\sqrt{D}\right) = a^2 - Db^2$.

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

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

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

Solution: Since K/F is Galois,

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

But $\tau \mapsto \tau\sigma$ just permutes the elements of $\mathrm{Gal}(K/F)$. Therefore $N(\beta) = N(\sigma(\beta))$. Thus $N(\beta/\sigma\beta) = N(\beta)/N(\sigma\beta) = 1$. Part (b) concerning the trace, which is not assigned, is similar.

Problem 14.3 #8. Determine the splitting field of the polynomial $x^p - x - a$ over $\mathbb{F}_p$, where $a \neq 0, a \in \mathbb{F}_p$. Show explicitly that the Galois group is cyclic. [See text for hint.]

Solution: We know from Exercise 5 in Section 13.5 (HW3) that the polynomial $f(x) = x^p - x - a$ is irreducible.

In the hint, α is supposed to be a root of $f(x)$. From the fact that $(\alpha+1)^p - (\alpha+1) = \alpha^p - \alpha = a$, we see that $\alpha + 1$ is also a root of f, so there is an automorphism σ of $\mathbb{F}(\alpha)$ that sends α to $\alpha+1$. Also, $E := \mathbb{F}_p(\alpha)$ contains p distinct roots of f, namely $\alpha, \alpha+1, \cdots, \alpha+p-1$, so E is the splitting field. Since $\deg(f) = p$, we have $[E : \mathbb{F}_p] = p$ and therefore $E = \mathbb{F}_{p^p}$. The automorphism σ has order p, hence $\mathrm{Gal}(E/\mathbb{F}_p)$ is cyclic, generated by σ.

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 σ_p, called the q-Frobenius automorphism.

(a) Prove that σ_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) (**not assigned**) Prove that every finite extension of $\mathbb{F}_q$ of degree n is cyclic with σ_q as a generator.

(d) (**not assigned**) 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 σ_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 $G = \mathrm{Gal}(E/F)$ has order $n = [E : F]$, and σ_q is an element. To show that it is cyclic with generator σ_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 $x^{q^m} - x$ 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.