WORKSHEET ON NORM, TRACE AND HILBERT 90 THEOREM, *505,* WINTER 2021

DUE TUESDAY, FEBRUARY 2; **ON GRADESCOPE**

Logistics: This worksheet will be graded as a usual homework, it will *not be peer reviewed.* The class time on Monday, February 1st, will be devoted to working on it with time for breakout rooms and questions.

Reading assignment. Part of this worksheet is an independent reading assignment. Read Theorem 7 in Section 14.2 in Dummit and Foote on "Linear independence of characters".

1. Norm and Trace

Let $F \subset K \subset L$ be a tower of finite extensions such that L/F is Galois. Let $G = \mathrm{Gal}(L/F)$ and $H = \mathrm{Gal}(L/K)$ (Note that $H < G$ is the subgroup of G corresponding to K via the Galois correspondence). Finally, let $\Sigma = \{\sigma : K \to \bar{F} : \sigma|_F = \mathrm{id}\}$, the set of field monomorphisms from K to $\bar{L}$ which leave F invariant.

Definition 1. For $\alpha \in K$, the *norm* of α over F is

$$N_{K/F}(\alpha) = \prod_{\sigma \in \Sigma} \sigma(\alpha).$$

Definition 2. For $\alpha \in K$, the *trace* of α over F is

$$\mathrm{Tr}_{K/F}(\alpha) = \sum_{\sigma \in \Sigma} \sigma(\alpha).$$

Lemma 3. *Suppose K/F is Galois. Then*

(1) $N_{K/F}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha)$.
(2) $\mathrm{Tr}_{K/F}(\alpha) = \sum_{\sigma \in \mathrm{Gal}(K/F)} \sigma(\alpha)$.

Proof. It suffices to show that if K is Galois (i.e. normal and separable) over F, then $\Sigma = \mathrm{Gal}(K/F)$. Recall that $\Sigma = \{\sigma : K \to \bar{F} : \sigma|_F = \mathrm{id}\}$ and $\mathrm{Gal}(K/F) = \mathrm{Aut}_F(K) = \{\sigma : K \xrightarrow{\sim} K : \sigma|_F = \mathrm{id}\}$. It is obvious that $\mathrm{Gal}(K/F) \subseteq \Sigma$, and for the other direction, we only need to show that every injective homomorphism $\sigma : K \to \bar{F}$ fixing F is actually an automorphism of K fixing F.

Well, since K is an algebraic extension of F, for every $\alpha \in K$, we have the minimal polynomial $\mathrm{Irr}(\alpha, F)$, where for every $\sigma : K \to \bar{F}$, $\sigma(\alpha)$ must also be a root of $\mathrm{Irr}(\alpha, F)$ (by properties of homomorphisms). As K is a normal extension, all roots of $\mathrm{Irr}(\alpha, F)$ are in K, so indeed σ can only possibly output in K. Since we specified that σ was injective, and now know that σ can only permute the roots of $\mathrm{Irr}(\alpha, F)$, of which there are only finitely many (for any given fixed α), σ must be surjective as well, implying that σ indeed is an automorphism of K.

Separability not needed to prove this fact (I think?); only necessary to ensure Galois group has "as many elements as possible", i.e. $[K : F]$ many. But this is not relevant here. □

The next proposition shows that norm and trace are operators which take an element in the field extension K/F *back* to the ground field F.

Proposition 4. *Norm and trace take elements in the field extension K/F back to the base field F*

(1) $N_{K/F}(\alpha) \in F$,
(2) $\mathrm{Tr}_{K/F}(\alpha) \in F$.

Proof. As we said in the proof of Prop. 3, the $\sigma \in \Sigma$ just permute the roots of $\mathrm{Irr}(\alpha, F)$; or focusing just on α, the $\sigma \in \Sigma$ just take α to some root of $\mathrm{Irr}(\alpha, F)$, say β. Of course, there are many different $\sigma \in \Sigma$ that take α to β — they just differ in what permuatations they do to the roots of other minimal polynomials and to the other roots of $\mathrm{Irr}(\alpha, F)$. But it is true that the number of $\sigma \in \Sigma$ (in total $|\Sigma|$ is finite because as we said at the top of this section, K is a finite extension, and there are only finitely many roots for each of the finitely many minimal polynomials that we have to determine positions for in order to determine σ on all of K) that take α to β is the same across all roots β of $\mathrm{Irr}(\alpha, F)$; we shall call this number N.

This is because how σ permutes the roots of one minimal polynomial is independent of how it permutes the roots of another minimal polynomial, and because the number of permutations of the roots of $\mathrm{Irr}(\alpha, F)$ that send α to β is the same regardless of what β is, because in all cases, once we decide $\alpha \mapsto \beta$, we still have $d-1$ roots left (where $d = \deg(\mathrm{Irr}(\alpha, F))$), where the 1st one has $(d-1)$ choices to map to, the 2nd one has $(d-2)$ choices, and so on. Anyways, we can now see that $N_{K/F}(\alpha) = (\prod_{\rho \in R} \rho)^N$ and $\mathrm{Tr}_{K/F}(\alpha) = N(\sum_{\rho \in R} \rho)$, where R is the set of roots of $\mathrm{Irr}(\alpha, F)$.

The final key to this puzzle is to notice that $\Pi_{\rho \in R}\rho$ and $\Sigma_{\rho \in R}\rho$ are just coefficents of $\mathrm{Irr}(\alpha, F)$ (up to multiples of -1) — the coefficients of the x^0 and x^{d-1} terms (times $(-1)^d$ and (-1) resp.) respectively (one can see this by writing $\mathrm{Irr}(\alpha, F) = \prod_{\rho \in R}(x - \rho)$, and expanding out, considering computations in the field K). As $\mathrm{Irr}(\alpha, F) \in F[x]$, it is clear that $N_{K/F}(\alpha)$ and $\mathrm{Tr}_{K/F}(\alpha)$ are simply powers or multiples of elements of F, implying that they too are in F. □

Proposition 5. *Norm is multiplicative:* $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$.

Proof. If σ is a homomorphism, $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$, so obviously

$$N_{K/F}(\alpha\beta) = \prod_{\sigma \in \Sigma} \sigma(\alpha\beta) = \prod_{\sigma \in \Sigma} \sigma(\alpha)\sigma(\beta) = \prod_{\sigma \in \Sigma} \sigma(\alpha) \prod_{\sigma \in \Sigma} \sigma(\beta) = N_{K/F}(\alpha)N_{K/F}(\beta).$$

□

Example 6. Let $K = F(\sqrt{D})$ be a quadratic extension, and let $\alpha = a + b\sqrt{D}$ for $a, b \in F$. Then $N_{K/F}(\alpha) = a^2 - Db^2$.

Proof. As it was specified that K is a quadratic extension, we have $\mathrm{Irr}(\sqrt{D}, F) = x^2 - D$. This is in fact a normal (two roots are $\pm\sqrt{D}$) and separable extension of F, where the only two automorphisms of K that fix F are the identity, and the one sending $\sqrt{D} \mapsto -\sqrt{D}$; we'll call them id and σ respectively. Thus, $N_{K/F}(\alpha) = \mathrm{id}(\alpha)\sigma(\alpha) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$, as desired. □

Example 7. Let K, $\sqrt{D}$, and α be as in Example 6. Then $\mathrm{Tr}_{K/F}(\alpha) = 2a$.

Proof. We already set up the context in Example 6, so $\mathrm{Tr}_{K/F}(\alpha) = \mathrm{id}(\alpha) + \sigma(\alpha) = (a + b\sqrt{D}) + (a - b\sqrt{D}) = 2a$, as desired. □

Proposition 8. *Trace is additive:* $\mathrm{Tr}_{K/F}(\alpha + \beta) = \mathrm{Tr}_{K/F}(\alpha) + \mathrm{Tr}_{K/F}(\beta)$

Proof. If σ is a homomorphism, $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$, so obviously

$$\mathrm{Tr}_{K/F}(\alpha\beta) = \sum_{\sigma \in \Sigma} \sigma(\alpha + \beta) = \sum_{\sigma \in \Sigma} \sigma(\alpha) + \sigma(\beta) = \sum_{\sigma \in \Sigma} \sigma(\alpha) + \sum_{\sigma \in \Sigma} \sigma(\beta) = \mathrm{Tr}_{K/F}(\alpha) + \mathrm{Tr}_{K/F}(\beta).$$

□

Proposition 9. *Let $\alpha \in K$ (a Galois extension of F), let $f(x) = \mathrm{Irr}(\alpha, F) = x^d + a_{d-1}x^{d-1} + \ldots + a_0$, and let $n = [K : F]$. Then*

(1) $N_{K/F}(\alpha) = (-1)^n a_0^{n/d} = ((-1)^d a_0)^{n/d}$.
(2) $\mathrm{Tr}_{K/F}(\alpha) = -\frac{n}{d}a_{d-1} = \frac{n}{d}((-1)a_{d-1})$

Proof. This basically amounts to proving that the N I talked about in the proof of Prop. 4 is actually equal to $\frac{n}{d}$. Recall that I defined N to be the number of $\sigma \in \Sigma$ that take α to β, where β is also a root of $\mathrm{Irr}(\alpha, F)$. Once we establish that $|\mathrm{Aut}(K/F)| = [K : F] = n$ (in this case where K is a Galois extension of F), then $|\Sigma| = n$ because we know from our proof of Lemma 3 that $\Sigma = \mathrm{Aut}(K/F)$. There are d possible choices to send α (d is the number of roots of $\mathrm{Irr}(\alpha, F)$ since it is separable), and we know from our proof of Prop. 4 that the number of $\sigma \in \Sigma$ sending α to any one of those choices is the same, implying that N is exactly $\frac{n}{d}$.

As for the identity $|\mathrm{Aut}(K/F)| = [K : F]$, note that $[K : F]_{\mathrm{sep}} = |\mathrm{Aut}(K/F)|$, so we just need to prove that for normal and separable extensions, $[K : F]_{\mathrm{sep}} = [K : F]$. Because K is a finite extension, we can write $K = F(\alpha_1, \ldots, \alpha_m)$. By Problem 2 of Homework 2 of 505, we have that

$$[K : F]_{\mathrm{sep}} = [K : F(\alpha_1, \ldots, \alpha_{m-1})]_{\mathrm{sep}} \cdots [F(\alpha_1) : F]_{\mathrm{sep}}.$$

Let's denote $E_i = F(\alpha_1, \ldots, \alpha_i)$, so $E_0 = F$ and $E_m = K$. If $\alpha_{i+1} \in E_i$, then $[E(\alpha_{i+1}) : E]_{\mathrm{sep}} = 1 = [E(\alpha_{i+1}) : E]$. Otherwise, $\alpha_{i+1} \in K \setminus E_i$. If we show that α_{i+1} is separable, then we know again from Problem 2 of Homework 2 that $[E(\alpha_{i+1}) : E]_{\mathrm{sep}} = [E(\alpha_{i+1}) : E]$, which will allow us to say that

$$[K : F]_{\mathrm{sep}} = [E_m : E_{m-1}]_{\mathrm{sep}} \cdots [E_1 : E_0]_{\mathrm{sep}} = [E_m : E_{m-1}] \cdots [E_1 : E_0] = [K : F].$$

Now to prove that "if". We formalize it in the following lemma: if K is a separable extension of F, E is an intermediate subfield of K, and $\alpha \in K \setminus E$, then indeed α must be separable over E. If not, then $\mathrm{Irr}(\alpha, E)$ would have multiple roots, but $\mathrm{Irr}(\alpha, E)$ divides $\mathrm{Irr}(\alpha, F)$ (since $\mathrm{Irr}(\alpha, F) \in F[x] \subseteq E[x]$ is also a polynomial in $E[x]$ with α as a root, and $\mathrm{Irr}(\alpha, E)$ is supposed to be minimal amongst such polynomials), implying that $\mathrm{Irr}(\alpha, F)$ must also have multiple roots; contradiction. □

Proposition 10. *For $a \in F$, $\alpha \in K$ (a Galois extension of F), we have*

(1) $N_{K/F}(a\alpha) = a^n N_{K/F}(\alpha)$,
(2) $\mathrm{Tr}_{K/F}(a\alpha) = a\,\mathrm{Tr}_{K/F}(\alpha)$.

Proof. We know our proof of Prop. 9 that $|\Sigma| = n$. Then because $\sigma \in \Sigma$ are homomorphisms that fix F,

$$N_{K/F}(a\alpha) = \prod_{\sigma\in\Sigma} \sigma(a\alpha) = \prod_{\sigma\in\Sigma} a\sigma(\alpha) = a^{|\Sigma|} \prod_{\sigma\in\Sigma} \sigma(\alpha) = a^n N_{K/F}(\alpha),$$

and similarly

$$\mathrm{Tr}_{K/F}(a\alpha) = \sum_{\sigma\in\Sigma} \sigma(a\alpha) = \sum_{\sigma\in\Sigma} a\sigma(\alpha) = a \sum_{\sigma\in\Sigma} \sigma(\alpha) = a\,\mathrm{Tr}_{K/F}(\alpha).$$

□

2. Hilbert 90 theorem

We formulate the multiplicative version of the Hilbert 90 theorem, for the norm. There is an analogous additive version for the trace - you could try stating it yourself or look it up. The statement of Hilbert 90 theorem is in fact a statement about vanishing of the first cohomology group, which is the formulation one can often find in the literature. We state it here explicitly without involving additional terminology.

Theorem 11. *Let K/F be a cyclic Galois extension of degree n (that is, the Galois group $\mathrm{Gal}(K/F)$ is cyclic group of order n) and let σ be a generator of $\mathrm{Gal}(K/F)$. For $\alpha \in K$, $N_{K/F}(\alpha) = 1$ if and only if there exists an element $\beta \in K$ such that $\alpha = \beta/\sigma(\beta)$.*

Proof. ($\Longleftarrow$): first, since σ is a homomorphism, we have that $\sigma(\beta)^{-1} = \sigma(\beta^{-1})$. Using multiplicativity of the norm, we have that

$$N_{K/F}(\alpha) = \prod_{i=1}^{n} \sigma^i(\beta) \prod_{i=1}^{n} \sigma^{i+1}(\beta^{-1}) = \prod_{i=1}^{n} \sigma^i(\beta) \prod_{i=1}^{n} \sigma^i(\beta^{-1}) = \prod_{i=1}^{n} \sigma^i(\beta\beta^{-1}) = \prod_{i=1}^{n} 1 = 1,$$

where like above $n = [K : F] = |\Sigma| =$ the order of the cyclic group $\mathrm{Gal}(K/F)$.

($\Longrightarrow$): for this direction, let us start with the simpler case of $n = 2$. As we assumed that $\mathrm{Gal}(K/F)$ is cyclic of order n with a generator σ, we have that $\sigma^2 = \mathrm{id}$. Let γ be any element in K, and define $\beta = \gamma + \alpha\sigma(\gamma)$. Then, $\sigma(\beta) = \sigma(\gamma) + \sigma(\alpha)\sigma^2(\gamma) = \sigma(\gamma) + \sigma(\alpha)\gamma$. Because we assumed that $N_{K/F}(\alpha) = \sigma(\alpha)\sigma^2(\alpha) = \sigma(\alpha)\alpha = 1$, it must be that $\sigma(\alpha) = \alpha^{-1}$. Thus, we have that $\alpha\sigma(\beta) = \alpha\sigma(\gamma) + \gamma = \beta$.

We're almost done with this case; we just need to show that $\sigma(\beta) \neq 0$ (for some $\gamma \in K$, we don't care which), which is of course equivalent to $\beta \neq 0$ (since σ is an isomorphism of K). To do this, we use Theorem 7 in Section 14.2 of D&F (the assigned reading at the beginning of this document), which tells us that because σ^0, σ^1 are distinct characters of $K^\times$ (i.e. homomorphisms from $G := K^\times$, which we are thinking of as a multiplicative group, to the multiplicative group $L^\times := K^\times$ of a field $L := K$), they are linearly independent, i.e. there are no a_0, a_1 s.t. $(a_0, a_1) \neq (0, 0)$ and $a_0\sigma^0 + a_1\sigma^1 = 0$ on all of $K^\times$. This gives the result since by linear independence and because $(1, \alpha) \neq (0, 0)$, there must be some $\gamma \in K$ s.t. $1\sigma^0(\gamma) + \alpha\sigma^1(\gamma) = \gamma + \alpha\sigma(\gamma) \neq 0$, as desired.

With this case down, it is pretty easy to extend to general n. Again because $\sigma^0, \ldots, \sigma^{n-1}$ are distinct, they are linearly independent, giving us that there is some γ s.t. the following expression is non-zero:

$$\sigma^0(\gamma) + \sigma^0(\alpha)\sigma^1(\gamma) + \sigma^0(\alpha)\sigma^1(\alpha)\sigma^2(\gamma) + \ldots + \prod_{i=0}^{n-2} \sigma^i(\alpha)\sigma^{n-1}(\gamma) = \sum_{j=1}^{n} \left(\prod_{i=0}^{j-2} \sigma^i(\alpha) \right) \sigma^{j-1}(\gamma).$$

Define this value to be β; then observe that (using multiplicity and additivity of homomorphisms)

$$\begin{aligned} \alpha \cdot \sigma(\beta) &= \alpha \cdot \left(\sum_{j=1}^{n} \left(\prod_{i=1}^{j-1} \sigma^i(\alpha) \right) \sigma^j(\gamma) \right) = \alpha \cdot \left(\sum_{j=1}^{n-1} \left(\prod_{i=1}^{j-1} \sigma^i(\alpha) \right) \sigma^j(\gamma) + \left(\prod_{i=1}^{n-1} \sigma^i(\alpha) \right) \sigma^n(\gamma) \right) \\ &= \alpha \cdot \left(\sum_{j=1}^{n-1} \left(\prod_{i=1}^{j-1} \sigma^i(\alpha) \right) \sigma^j(\gamma) + \alpha^{-1}\gamma \right) = \sum_{j=2}^{n} \left(\prod_{i=0}^{(j-1)-1} \sigma^i(\alpha) \right) \sigma^{j-1}(\gamma) + \gamma = \beta. \end{aligned}$$

We said in the $n = 2$ case that $\beta \neq 0 \iff \sigma(\beta) \neq 0$, and that remains true here, so indeed we can divide by $\sigma(\beta)$ to get that $\alpha = \beta/\sigma(\beta)$, for the $\beta \in K$ defined above, as desired. □