MATH 552 NOTES – LECTURE 7

Let E/K be Galois, with finite Galois group G.

Definition 1 (Trace). The *trace map* $\mathrm{tr} : E \to K$ is $\mathrm{tr}(u) = \sum_{g \in G} g(u)$. (This is an element of K since $g(\mathrm{tr}(u)) = \mathrm{tr}(u)$ for all u.) It is a linear transformation of the underlying K-vector spaces, as $\mathrm{tr}(u+v) = \mathrm{tr}(u)+\mathrm{tr}(v)$ and $\mathrm{tr}(au) = a\,\mathrm{tr}(u)$ for $a \in K$.

The following result shows that $\mathrm{tr} = \sum g$ is nonzero, and hence a surjection. This is clear if $\mathrm{char}(E)$ doesn't divide $n = [E : K]$, as $\mathrm{tr}(1/n) = 1$.

Proposition 2. *Let $g_1, ..., g_n$ be distinct automorphisms of a field E. Then the g_i are linearly independent in the sense that for $a_i \in E$, if $\sum a_i(g_i(u)) = 0$ for every $u \in E$, then all the a_i are zero.*

Proof. If the g_i were linearly dependent, pick a dependence relation with as many 0's as possible, say $\sum_{i=1}^{m} a_i(g_i(u)) = 0$ for all $u \in E$. Clearly $m \neq 1$, and since $g_1 \neq g_2$ there is a $v \in E$ so $g_1(v) \neq g_2(v)$. Replacing u by vu, we get $\sum a_i g_i(v) g_i(u) = 0$; subtracting $g_1(v) \sum a_i\, g_i(u) = 0$ we get a shorter relation, contradicting linear dependence:

$$a_2\,[g_2(v) - g_1(v)]\, g_2(u) + \cdots + a_m\,[g_m(v) - g_1(v)]\, g_m(u) = 0. \qquad \square$$

Definition 3. We say that a sequence of vector spaces $V_0 \xrightarrow{i} V_1 \xrightarrow{j} V_2$ is *exact* if $V_0 \xrightarrow{ji} V_2$ is zero and the image of i is $\ker(j)$. For example, if $\mathrm{Gal}(E/K)$ is cyclic with generator γ then $0 \to K \to E \xrightarrow{\gamma-1} E$ is exact.

Theorem 4. *Suppose that $G = \langle \gamma \rangle$ is a cyclic group. Then an element $u \in E$ has trace 0 iff $u = v - \gamma(v)$ for some $v \in E$. There is an exact sequence*

$$0 \to K \to E \xrightarrow{\gamma-1} E \xrightarrow{\mathrm{tr}} K \to 0.$$

Proof. It is clear that each of the compositions are zero, and that the sequence is exact except possibly at the second E. A count of dimensions shows that the image V of $E \xrightarrow{\gamma-1} E$ has $\dim_K(V) = \dim_K(E) - 1$, and $\dim_K \ker(E \xrightarrow{\mathrm{tr}} K) = \dim_K(E) - 1$. Hence the sequence is also exact at the second E. $\square$

Date: Feb. 14, 2025.

Corollary 5. *If* $\operatorname{char}(K) = p$ *and* E/K *is Galois with* $[E : K] = p$*, then* $E = K(u)$*, where* u *is a root of* $t^p - t - a$ *for some* $a \in K$*.*

Proof. Let γ generate $\operatorname{Gal}(E/K)$. By Theorem 4, since $\operatorname{tr}(1) = p = 0$, $1 = \gamma(u) - u$ for some $u \in E$, i.e., $\gamma(u) = 1 + u$. Hence $\gamma(u^p) = (1+u)^p = 1 + u^p$. So $\gamma(u^p - u) = u^p - u$, which implies that $a = u^p - u \in K$. Since $u \notin K$ and there are no intermediate subfields, $E = K(u)$, and $t^p - t - a$ must be the minimal polynomial of u. □

Definition 6 (Norm). The *norm map* $N = N_{E/K} : E^\times \to K^\times$ is $N(u) = \prod_{g \in G} g(u)$. Note that $N(u)$ is in $K^\times$ since $g(N(u)) = N(u)$ for all u. The norm is a homomorphism of abelian groups.

The prototype is the norm map $\mathbb{C}^\times \to \mathbb{R}^\times$ sending $z = x + iy$ to $|z|^2 = x^2 + y^2$. Similarly, $N : \mathbb{Q}(\sqrt{d})^\times \to \mathbb{Q}^\times$ sends $u = a + b\sqrt{d}$ to $N(u) = a^2 - d\,b^2$. The equations $a^2 - d\,b^2 = 1$ and more generally $a^2 - d\,b^2 = c$ are called *Pell's equation* and were studied by Diophantus (in Greece) around 250 AD, and by Brahmagupta (in India) around 628 AD. The following result, due to Kummer, is usually called "*Hilbert's Theorem 90*" since it was the 90^{th} theorem in Hilbert's survey of number theory in 1897.

Theorem 7 (Hilbert's Theorem 90)**.** *Suppose that the Galois group* $G = \langle \gamma \rangle$ *is a cyclic group. Then an element* $u \in E^\times$ *has norm 1 iff* $u = \gamma(v)/v$ *for some* $v \in E^\times$*. There is an exact sequence*

$$1 \to K^\times \to E^\times \xrightarrow{\gamma - 1} E^\times \xrightarrow{N} K^\times$$

(The cokernel of N is the cohomology group $H^2(G, E^\times)$.

Proof. Again, it is easy to check exactness everywhere except at the second $E^\times$; since $N(\gamma(v)/v) = 1$, it suffices to suppose that $N(u) = 1$ and find a v such that $u = \gamma(v)/v$.

Write $x_0 = uy$, $x_1 = u(\gamma u)(\gamma y)$ and

$$x_i = x_i(y) = \left\{ u\,(\gamma u)(\gamma^2 u) \cdots (\gamma^i u) \right\} \gamma^i y. \quad i = 0, ..., n-1.$$

Since $N(u) = 1$, $x_{n-1} = \gamma^{n-1} u$. For $i = 0, ..., n-2$ we also have $x_{i+1} = u(\gamma x_i)$, or $\gamma(x_i) = u^{-1} x_{i+1}$. By Proposition 2, there is a $y \in E$ such that $v = x_0 + x_1 + \cdots + x_{n-1}$ is nonzero. Then

$$\gamma(v) = \sum\nolimits_{i=0}^{n-1} \gamma(x_i) = u^{-1} \left(x_1 + x_2 + \cdots + x_{n-1}\right) + \gamma^n(y).$$

Since $\gamma^n = 1$, $\gamma^n(y) = y = x_0/u$. Hence $\gamma(v) = v/u$, as required. □

Corollary 8. *Suppose that* $\mathrm{Gal}(E/K) = \langle\gamma\rangle$ *is cyclic of order* n*,* $1/n \in K$ *and* $\mu_n \subset K^\times$*. Then* $E = K(u)$*, where* u *has minimal polynomial* $t^n - a$ *for some* $a \in K$*.*

Proof. Let ω be a primitive n^{th} root of unity in K. Since $N(\omega) = \omega^n = 1$, there is a $v \in E$ so that $\omega = \gamma(v)/v$. Then $\gamma(v) = \omega v$ and $\gamma(v^n) = \omega^n v = v$. Since $a = v^n$ is invariant under γ, it lies in K and v satisfies $t^n - a = 0$.

Since $t^n - a = \prod_i (t - \omega^i v)$, $K(v)$ is a splitting field of $t^n - a$ over K. This is the minimal polynomial of v, because that the automorphisms $I, \gamma, ..., \gamma^{n-1}$ of E permute the roots of $t^n - a$. □

Theorem 9. *Let* K *be a field of characteristic 0, and* E/K *a Galois extension with Galois group* G*. If* G *is solvable, then* E *can be embedded in a radical extension of* K*.*

Proof. We proceed by induction on $[E : K]$. Pick a normal subgroup H of the solvable group G with $[G : H] = p$ and let E_1 be a splitting field of $t^p - 1$ over E. Then E_1/K is still Galois with solvable Galois group; E_1 is also Galois over $K_1 = K(\mu_p)$. Since K_1 is a radical extension of K, it suffices to show that E_1 is a radical extension of K_1. In addition, $\mathrm{Gal}(E_1/K_1)$ is isomorphic to a subgroup of G, by the map restricting an automorphism g of E_1 to its restriction to E. (If g fixes E and μ_p, it fixes E_1.) If $\mathrm{Gal}(E_1/K_1) \neq G$, we sre done by induction.

Thus it suffices to assume that $K = K(\mu_n)$ and $E = E(\mu_n)$. Let $L = H'$ be the intermediate subfield of E_1 corresponding to H. Since $H \lhd G$ and $[L : K] = p$, L/K is Galois and $\mu_p \subset K$, so $L = K(u)$ with the minimal polynomial of u of the form $t^p - a$. (See Corollary 3 of the Lecture 5 notes.) By induction on $[E : K]$, E can be embedded in a radical extension of K which, as we have seen, is a radical extension of K. □

Exercises:

1) If E/K is Galois, and $[E : K] < \infty$, show that $\mathrm{tr} : E \to K$ is onto.
2) Let K be a field of characteristic $p > 0$. Prove that $t^p - t - a$ is either irreducible or factors completely in K. *Hint:* Consider $g(t) = t + 1$.
3) Prove Hilbert's Theorem 90 when E/K is normal but not Galois.