21-238, Math Studies Algebra 2, Department of Mathematical Sciences, Carnegie Mellon University
Spring 2012: Monday, Wednesday, Friday, 10:30 am, Doherty Hall 1211.
Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

41- Friday May 4, 2012.

Lemma 41.1: One writes φ_n for the Frobenius operator $a \mapsto a^p$ on K_n. Every $\sigma \in Aut_E(F)$ is characterized by a sequence of integers a_n with $0 \leq a_n < n$ for all $n \geq 1$ and $a_n = a_m \pmod m$ whenever n is a multiple of m, and such that $\sigma|_{K_n} = \varphi_n^{a_n}$.
Proof: Since K_n is a splitting field extension of E, it is a normal extension of E, the restriction of σ to K_n belongs to $Aut_E(K_n)$, so that it is $\varphi_n^{a_n}$ for some integer a_n, but since $\varphi_n^n = id_{K_n}$, one may impose $0 \leq a_n < n$. Then, if n is a multiple of m, the restriction of $\varphi_n^{a_n}$ to K_m must be $\varphi_m^{a_m}$, but since φ_n restricted to K_m is φ_m, it means that $a_n = a_m \pmod m$.

Conversely, let b_n be a sequence of integers satisfying $0 \leq b_n < n$ for all $n \geq 1$ and $b_n = b_m \pmod m$ whenever n is a multiple of m; one defines τ on F by $\tau(z) = \big(\varphi_n(z)\big)^{b_n}$ if $z \in K_n$, and the definition makes sense since if $z \in K_i \cap K_j$, then for $k = i\,j$ one has $\big(\varphi_i(z)\big)^{b_i} = \big(\varphi_k(z)\big)^{b_k}$ because i divides k, and $\big(\varphi_k(z)\big)^{b_k} = \big(\varphi_j(z)\big)^{b_j}$ because j divides k, hence $\big(\varphi_i(z)\big)^{b_i} = \big(\varphi_j(z)\big)^{b_j}$.

Lemma 41.2: There are uncountably many sequences a_n, characterized by their values for $n = m!$ for all m.

If $\sigma, \tau \in Aut_E(F)$ are associated to sequences a_n, b_n, then $\tau \circ \sigma$ is associated to the sequence c_n with $c_n = a_n + b_n \pmod n$.
Proof: It is sufficient to know a_n for an increasing sequence of integers $n = k_1, k_2, \ldots$ with $k_m \to \infty$ as $m \to \infty$ if it has the property that for each integer i there is at least one k_j which is a multiple of i; an example is $k_j = j!$ for all $j \geq 1$. Once $a_{m!}$ is given with $0 \leq a_{m!} < m!$, one must take $a_{(m+1)!} = a_{m!} + \ell_m m!$ with $0 \leq \ell_m \leq m$, so that $a_{(m+1)!} = \sum_{j=1}^m \ell_j j!$; of course, with more than two choices for each integer ℓ_m, one creates an uncountable set.

For $z \in K_n$, one has $\tau \circ \sigma(z) = \big(z^{p^{a_n}}\big)^{p^{b_n}} = z^{p^{a_n} p^{b_n}} = z^{p^{a_n+b_n}}$.

Definition 41.3: A subset $X \subset Aut_E(F)$ is said to be *open* if and only if for all $\sigma \in X$ there exists n such that $\tau \in Aut_E(F)$ and $\tau|_{K_n} = \sigma|_{K_n}$ imply $\tau \in X$.

A subset $Y \subset Aut_E(F)$ is said to be *closed* if and only if whenever $\sigma \in Aut_E(F)$ is such that for all n there exists $\tau \in Y$ with $\tau|_{K_n} = \sigma|_{K_n}$, then $\sigma \in Y$.

Lemma 41.4: Definition 41.3 defines a topology on $Aut_E(F)$, which is Hausdorff (and even normal), and makes $Aut_E(F)$ a compact topological group, with a basis of (open) neighbourhoods of id_F made of open subgroups.
Proof: An arbitrary union of open subsets is clearly open, so one must only check that if X_1 and X_2 are open, then $X_1 \cap X_2$ is open: for $\sigma \in X_1 \cap X_2$, there exist n_1, n_2 such that, for $\tau \in Aut_E(F)$, $\tau|_{K_{n_1}} = \sigma|_{K_{n_1}}$ implies $\tau \in X_1$, and $\tau|_{K_{n_2}} = \sigma|_{K_{n_2}}$ implies $\tau \in X_2$; one then chooses $n = n_1 n_2$ (or any multiple of both n_1 and n_2), so that $\tau|_{K_n} = \sigma|_{K_n}$ implies both $\tau|_{K_{n_1}} = \sigma|_{K_{n_1}}$ and $\tau|_{K_{n_2}} = \sigma|_{K_{n_2}}$ since n is a multiple of n_1 and a multiple of n_2, hence $\tau \in X_1 \cap X_2$. The definition of a subset of $Aut_E(F)$ being closed then corresponds to its complement being open.

For the topology to be Hausdorff, for all $\sigma_1, \sigma_2 \in Aut_E(F)$ with $\sigma_1 \neq \sigma_2$, one must find an open set X_1 containing σ_1 and an open set X_2 containing σ_2 with $X_1 \cap X_2 = \emptyset$: there exists n such that $\sigma_2|_{K_n} \neq \sigma_1|_{K_n}$, and then $X_1 = \{\tau \in Aut_E(F) \mid \tau|_{K_n} = \sigma_1|_{K_n}\}$ and $X_2 = \{\tau \in Aut_E(F) \mid \tau|_{K_n} = \sigma_2|_{K_n}\}$ satisfy these conditions. That the topology is normal follows from showing that it is a compact space, since every compact Hausdorff space is normal.

To be a topological group, addition and inverse must be continuous. For $\sigma, \tau \in Aut_E(F)$, an open set around $\tau \circ \sigma$ contains a particular open set $C = \{\rho \in Aut_E(F) \mid \rho|_{K_n} = \tau \circ \sigma|_{K_n}\}$, so that if one considers the open set $A = \{\sigma' \in Aut_E(F) \mid \sigma'|_{K_n} = \sigma|_{K_n}\}$ around σ and the open set $B = \{\tau' \in Aut_E(F) \mid \tau'|_{K_n} = \tau|_{K_n}\}$ around τ, then $\sigma' \in A$ and $\tau' \in B$ imply $\tau' \circ \sigma' \in C$. For the continuity of the inverse, one notices that for $\rho \in Aut_E(F)$ the condition $\rho|_{K_n} = \sigma|_{K_n}$ is equivalent to $\rho^{-1}|_{K_n} = \sigma^{-1}|_{K_n}$.

For $0 \leq a < m$, one defines the open set $A(m;a) = \{\sigma \in Aut_E(F) \mid \sigma|_{K_m} = \varphi_m^a\}$, noticing that $A(n;b) \subset A(m;a)$ if m divides n and $b = a \pmod m$. Given a covering of $Aut_E(F)$ by a family of open sets

$U_i, i \in I$, one considers the set Z of all pairs (m, a) with $A(m; a) \subset U_i$ for some $i \in I$, and the claim is that there exists N such that all (N, a) belongs to Z for $a = 0, \ldots, N-1$, so that a finite family of U_i contain these $A(N; a)$ and form a finite open subcovering, showing that $Aut_E(F)$ is compact: since the restriction of any $\sigma \in Aut_E(F)$ is characterized by its restrictions to $K_{m!}$, for all m, one creates a graph with an edge up from $(m!; a)$ to $\big((m+1)!, b\big)$ if $b = a \pmod{m!}$, so that if $(m!, a) \in Z$ then all the vertices above also belong to Z; then, for each $(m!, a) \in Z$ one erases all the edges above this point, i.e. one keeps only the vertices in Z which are minimal elements for the order described, and the claim is that one has erased all the edges above some level N. If it was not true, there would exist an infinite path along edges upward (a special case of König's lemma),[1,2] corresponding to an element $\sigma \in Aut_E(F)$, which would belong to some U_i, hence there would be a level n with $\sigma|_{K_n} = \varphi_n^a$ and $A(n, a) \subset U_i$, and for $m! \geq n$ the corresponding point $(m!, b)$ would belong to Z, and the path upward would have been erased, hence it could not be infinite.

id_F corresponds to the sequence $a_n = 0$ for all n, and a basis of open sets containing 0 is given by the $A(m; 0)$ for all m, and one notices that $A(m; 0)$ is a subgroup of $Aut_E(F)$.

Lemma 41.5: If K is an intermediate field, then $H = Aut_K(F)$ is a closed subgroup of $Aut_E(F)$. One has $Fix(H) = K$, and every closed subgroup has this form.[3]
Proof: Since $K \cap K_n$ is a subfield of K_n it must be K_m for some m dividing n, so that K is the union of some K_m (those which are included in K, of course). If $\sigma \in Aut_E(F)$, it fixes K if and only if for each n it fixes $K_m = K \cap K_n$, i.e. the sequence associated with σ has a_n belonging to a subgroup of $\mathbb{Z}_n$. Such a subgroup H of $Aut_E(F)$ is closed, since by Definition 41.3, for arbitrary subsets $X_n \subset \{0, 1, \ldots, n-1\}$ for $n \geq 1$, if one denotes $Y_n = \{\varphi_n^a \mid a \in X_n\}$, the subset of $Aut_E(F)$ defined by $\{\sigma \in Aut_E(F) \mid \sigma|_{K_n} \in Y_n$ for all $n \geq 1\}$ is closed, and every closed subset $Z \subset Aut_E(F)$ has this form, with $Y_n = \{\tau|_{K_n} \mid \tau \in Z\}$. Then a closed subgroup must be such that each Y_n is a subgroup, and is then associated with an intermediate field.

---

[1] Dénes König, Hungarian mathematician, 1884–1944. He worked in Budapest, Hungary.

[2] A special case of König's lemma is that every tree which contains infinitely many vertices, each having finite degree, has at least one infinite simple path.

[3] There are subgroups which are not closed: if $\sigma_0 \in Aut_E(F)$ is defined by the sequence $a_n = 1$ for all $n \geq 2$ (and a_1 must be 0), then it generates an infinite cyclic group which is not closed, but is dense (its closure is $Aut_E(F)$).