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

32- Wednesday April 11, 2012.

Lemma 32.1: If a field extension F of E is finite and normal, it is a splitting field extension for some $f \in E[x]$.
Proof: If $[F\,{:}\,E] = m+1$ and $1, a_1, \ldots, a_m$ is a basis of F as an E-vector space, let $P_{a_1}, \ldots, P_{a_m} \in E[x]$ be the monic irreducible polynomials (which split over F) associated to $a_1, \ldots, a_m$, and define $f = P_{a_1} \cdots P_{a_m}$. Then $f \in E[x]$ splits over F, and its roots generate F (since they contain $\{a_1, \ldots, a_m\}$), so that F is a splitting field extension for f over E.

Lemma 32.2: If F is a splitting field extension for $f \in E[x]$ over E, then it is a normal extension.
Proof: If $deg(f) = d$, then one has $[F\,{:}\,E] \le d!$. For $a \in F$, let $P_a \in E[x]$ be its associated monic irreducible polynomial, and let $\widetilde{F}$ be a splitting field extension for P_a over F; if one shows that $\widetilde{F} = F$, it implies that P_a splits over F, and since a is arbitrary, then F is a normal extension.

Since $\widetilde{F}$ is generated by the roots of P_a, one must show that the roots of P_a belong to F. Let $b \in \widetilde{F}$ with $P_a(b) = 0$, so that P_a is the monic irreducible polynomial associated to b, and then $E(a)$ and $E(b)$ satisfy $[E(a)\,{:}\,E] = [E(b)\,{:}\,E] = deg(P_a)$, and $E(b)$ is isomorphic to $E(a)$.[1] Then, one observes that $F(b)$ is a splitting field extension for f over $E(b)$,[2] but F is also a splitting field extension for f over $E(a)$,[3] and by the uniqueness of splitting field extensions (up to isomorphism) one has $[F(b) : E(b)] = [F : E(a)]$; from $[F(b) : E] = [F(b) : F]\,[F : E(a)]\,[E(a) : E]$ and $[F(b) : E] = [F(b) : E(b)]\,[E(b) : E]$, one deduces that $[F(b)\,{:}\,F] = 1$, so that $b \in F$.

Lemma 32.3: Let G be a group and let F be a field. Then, the characters of G in F form a F-linearly independent set in the F-vector space F^G of all functions from G into F.
Proof: One assumes that a F-linearly dependent set of characters exists, and one chooses one with the minimum number n of elements, and $n > 1$ since a character cannot be 0, because it maps $e \in G$ onto 1: one has $\sum_{i=1}^n \lambda_i \varphi_i = 0$, i.e. $\sum_{i=1}^n \lambda_i \varphi_i(g) = 0$ for all $g \in G$, with distinct characters $\varphi_1, \ldots, \varphi_n$, and none of the $\lambda_i \in F$ is 0. Since $\varphi_n \ne \varphi_1$, there exists $h \in G$ such that $\varphi_n(h) \ne \varphi_1(h)$, and then $0 = \sum_{i=1}^n \lambda_i \varphi_i(h\,g) = \sum_{i=1}^n \lambda_i \varphi_i(h)\,\varphi_i(g)$, so that by subtracting $\varphi_n(h) \sum_{i=1}^n \lambda_i \varphi_i(g) = 0$ one obtains $\sum_{i=1}^{n-1} \lambda_i\big(\varphi_i(h) - \varphi_n(h)\big)\,\varphi_i(g) = 0$ for all $g \in G$: it means that $\sum_{i=1}^{n-1} \mu_i\,\varphi_i = 0$ with $\mu_i = \lambda_i\big(\varphi_i(h) - \varphi_n(h)\big)$ for $i = 1, \ldots, n-1$, and $\mu_1 \ne 0$, contradicting the minimality of n.

Lemma 32.4: For a field F, $Aut(F)$ is an F-linearly independent set of F^F.
Proof: Each element of $Aut(F)$, when restricted to F^* is a character of $G = F^*$ in F, and one applies Lemma 32.3.

Lemma 32.5: If F is a finite field extension of E, then $|Aut_E(F)| \le [F\,{:}\,E]$.
Proof: If $[F\,{:}\,E] = n$, F is an E-vector space of dimension n, and one chooses a basis $f_1, \ldots, f_n$ of F. Suppose that σ_j, $j = 1, \ldots, n+1$ are distinct elements of $Aut_E(F)$, and let $w_j = \big(\sigma_j(f_1), \ldots, \sigma_j(f_n)\big) \in F^n$, so that the elements $w_1, \ldots, w_{n+1}$ are F-linearly dependent (since the dimension of F^n is n), and $\sum_{j=1}^{n+1} \lambda_j w_j = 0$ (i.e. $\sum_{j=1}^{n+1} \lambda_j \sigma_j(f_i) = 0$ for $i = 1, \ldots, n$), not all λ_j being 0. By E-linearity, one has $\sum_{j=1}^{n+1} \lambda_j \sigma_j(f) = 0$ for all $f \in F$,[4] and since it holds for all $f \in F$, one has $\sum_{j=1}^{n+1} \lambda_j \sigma_j = 0$, which contradicts Lemma 32.4.

[1] If $d = deg(P_a)$, the isomorphism sends $c_0 + c_1 a + \ldots + c_{d-1} a^{d-1}$ to $c_0 + c_1 b + \ldots + c_{d-1} b^{d-1}$ for all $c_0, c_1, \ldots, c_{d-1} \in E$.

[2] Because f splits in F, it splits in $F(b)$, and the smallest field containing the roots of f and $E(b)$ must contain the roots of f and E, so that it contains F (since F is a splitting field extension for f over E), and then it must contain $F(b)$ because it contains b.

[3] A splitting field extension F for f over E is a splitting field extension for f over any intermediate field K, since f splits in F, and a field containing the roots of f and K contains the roots of f and E, hence F.

[4] For $f \in F$, one has $f = \sum_{i=1}^n e_i f_i$ for some $e_1, \ldots, e_n \in E$, and it implies that $\sum_{j=1}^{n+1} \lambda_j \sigma_j(f) = \sum_{j=1}^{n+1} \sum_{i=1}^n \lambda_j \sigma_j(e_i f_i) = \sum_{j=1}^{n+1} \sum_{i=1}^n \lambda_j \sigma_j(e_i)\,\sigma_j(f_i)$ since the σ_i are homomorphisms, which is equal to $\sum_{j=1}^{n+1} \sum_{i=1}^n \lambda_j e_i \sigma_j(f_i)$ since the σ_i fix E, i.e. $= \sum_{i=1}^n e_i\big(\sum_{j=1}^{n+1} \lambda_j \sigma_j(f_i)\big) = 0$.

Lemma 32.6: If F is a field and H is a finite subgroup of $Aut(F)$, then the field $E = Fix(H)$ satisfies $[F\!:\!E] = |H|$ and $Aut_E(F) = H$ (so that F is a Galois extension of E).

Proof: It suffices to show that $[F\!:\!E] \leq |H|$, since $H \leq Aut_E(F)$ implies $|H| \leq |Aut_E(F)|$, which is $\leq [F\!:\!E]$ because F is a finite extension of E (Lemma 32.5), and equality must hold.

Let $H = \{\sigma_1, \ldots, \sigma_m\}$ with $\sigma_1 = id$; the case $m = 1$ is true, since $E = F$ in this case. One assumes that $m > 1$ and that one can find $f_1, \ldots, f_{m+1} \in F$ which are E-linearly independent, and one sets $v_i = \big(\sigma_1(f_i), \ldots, \sigma_m(f_i)\big) \in F^m$ for $i = 1, \ldots, m+1$, which are then F-linearly dependent (since F^m has dimension m), and distinct (because the first entry of v_i is f_i). Let N be minimal such that there is a F-linear dependence among N of the v_i, and using a permutation on $\{1, \ldots, m+1\}$ one may assume that $\sum_{i=1}^N \lambda_i v_i = 0$ with all λ_i non-zero, and (by multiplying by λ_1^{-1}) one may assume that $\lambda_1 = 1$. Since the first entry of v_i is f_i, and the f_i are E-linearly independent, one deduces that some λ_i does not belong to E, and by a permutation on $\{2, \ldots, N\}$ one may assume that $\lambda_N \notin E$, and by a permutation on $\{\sigma_2, \ldots, \sigma_m\}$ one may assume that $\sigma_m(\lambda_N) \neq \lambda_N$ (because of the definition of E, that elements in F fixed by $\sigma_1, \ldots, \sigma_m$ belong to E). Then, $\sum_{i=1}^N \lambda_i v_i = 0$ means $\sum_{i=1}^N \lambda_i \sigma_j(f_i) = 0$ for $j = 1, \ldots, m$, and applying σ_m gives $\sum_{i=1}^N \sigma_m(\lambda_i)\, \sigma_m\big(\sigma_j(f_i)\big) = 0$ for $j = 1, \ldots, m$, but since H is a group, the $\sigma_m \circ \sigma_j$ run through H and it is then equivalent to $\sum_{i=1}^N \sigma_m(\lambda_i)\, \sigma_j(f_i) = 0$ for $j = 1, \ldots, m$, i.e. $\sum_{i=1}^N \sigma_m(\lambda_i)\, v_i = 0$; after subtracting and using $\sigma_m(\lambda_1) = \lambda_1$ and $\sigma_m(\lambda_N) \neq \lambda_N$, one finds a shorter non trivial F-dependence among the v_i, contradicting the minimality of N.