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

33- Friday April 13, 2012.

Lemma 33.1: If F is a finite field extension of E, it is a Galois extension of E if and only if $|Aut_E(F)| = [F:E]$.
Proof: If $H = Aut_E(F)$, then H is finite by Lemma 32.5, and then $K = Fix(H)$ is an intermediate field, which satisfies $[F:K] = |H|$ by Lemma 32.6. If F is a Galois extension of E, it means that $K = E$, hence $[F:E] = |H|$. Conversely, if $[F:E] = |H|$, then $[F:E] = [F:K]\,[K:E]$ gives $[K:E] = 1$, i.e. $K = E$.

Definition 33.2: If E is a field and $P \in E[x]$ is *irreducible*, then P is called *separable* over E if and only if P has *no repeated root in any extension field* F of E.

Lemma 33.3: If E is a field and $P \in E[x]$ is irreducible, then P is separable if and only if it has no repeated root in one splitting field extension F for P over E.
Proof: One assumes that P has no repeated root in F, but that it has a repeated root b in an extension field G of E. Let H be a splitting field extension for P over G, and let $F_0 = E(r_1, \ldots, r_k) \subset H$ where $r_1, \ldots, r_k$ are the roots of P in H. F_0 is a splitting field extension for P over E, and by uniqueness of the splitting field extension up to isomorphism, there is an isomorphism σ of F_0 onto F which extends id_E, and since b is a repeated root of P in F_0, $\sigma(b)$ is a repeated root of P in F,[1] a contradiction.

Lemma 33.4: If E is a field, if $P \in E[x]$ is irreducible, and if $P' \neq 0$, then P is separable. In particular, in a field of characteristic 0, every non-zero irreducible polynomial is separable.
Proof: Since E is a field, $E[x]$ is a PID, so that the ideal (P, P') is generated by a (non-zero) element $d \in E[x]$. Because d divides P, and P is irreducible, d is a unit or an associate of P, in which case it could not divide P' (since $deg(P') \leq deg(P) - 1$), so that d is a unit which can be taken to be 1, i.e. there exist $A, B \in E[x]$ such that $A\,P + B\,P' = 1$. Then, the same equation holds in $G[x]$ for any extension field G, and one cannot have a repeated root b, since it would imply $0 = A(b)\,P(b) + B(b)\,P'(b) = 1$.

Definition 33.5: A non-zero polynomial is *separable* if and only if its irreducible factors are separable.

In an extension field F of E, an element $a \in F$ is *separable* if and only if it is algebraic over E, and its minimal (monic irreducible) polynomial $P_a \in E[x]$ is separable.

An extension field F of E is *separable* if and only if it is an algebraic extension, and every $a \in F$ is separable.

Lemma 33.6: If $P \in E[x]$ is separable over E, and F is a field extension of E, then P is separable over F.
Proof: Let $Q \in F[x]$ be an irreducible factor of P, and assume that it has a repeated root in a field extension G of F. Let $P = P_1 \cdots P_n$ be the factorization into irreducible factors in $E[x]$ (and the factorization holds in $F[x]$, although the factors may not be irreducible in $F[x]$); since $F[x]$ is a PID, Q is prime in $F[x]$,[2] so that Q must divide P_i for some i (i.e. $P_i = Q\,R$ for some $R \in F[x]$), but this implies that P_i has a repeated root in G, which is a field extension of E, a contradiction.

Lemma 33.7: Let F be a finite field extension of E, and let $a \in F$. Let k be the number of distinct elements of the form $\sigma(a)$ for $\sigma \in Aut_E(F)$, and let ℓ be the number of distinct roots in F of the minimal (monic irreducible) polynomial $P_a \in E[x]$. Then, $k \leq \ell \leq [E(a):E]$ and $|Aut_E(F)| = k\,|Aut_{E(a)}(F)|$.
Proof: One has $\ell \leq deg(P_a) = [E(a):E]$. One has $P_a(a) = 0$, and for every $\sigma \in Aut_E(F)$ one has $P_a\big(\sigma(a)\big) = 0$, so that the elements $\sigma(a)$ are among the roots of P_a,[3] and $k \leq \ell$. $Aut_{E(a)}(F)$ is a subgroup of

[1] If $f_0 = \sum_n c_n x^n \in F_0[x]$ its image is $f = \sigma(f_0) = \sum_n \sigma(c_n) x^n$, so that $\sigma\big(f_0(a)\big) = f\big(\sigma(a)\big)$ for all $a \in F_0$, since σ is an isomorphism; a consequence is that if a is a root of f_0, then $\sigma(a)$ is a root of f. Because $\sigma(n\,c_n) = \sigma(c_n + \ldots + c_n) = \sigma(c_n) + \ldots + \sigma(c_n) = n\,\sigma(c_n)$, one finds that $\sigma(f_0') = f'$, and a consequence is that if a is a root of f_0', then $\sigma(a)$ is a root of f'.

[2] It is also true in a UFD that every irreducible element is prime.

[3] If $Q = c_0 + c_1 x + \ldots \in E[x] \subset F[x]$, and $\sigma \in Aut(F)$ then $R = \sigma(Q) \in F[x]$ is the polynomial $R = \sigma(c_0) + \sigma(c_1)\,x + \ldots$, so that for all $a \in F$ one has $\sigma\big(Q(a)\big) = R\big(\sigma(a)\big)$: if a is a root of Q, then $\sigma(a)$ is a root of R. It is the fact that $\sigma \in Aut_E(F)$ (i.e. σ fixes E) which gives $R = Q$.

$Aut_E(F)$, which is then a union of left cosets of $Aut_{E(a)}(F)$, each with size $|Aut_{E(a)}(F)|$; for $\sigma, \tau \in Aut_E(F)$ one has $\sigma(a) = \tau(a)$ if and only if $\tau^{-1}\sigma(a) = a$, i.e. if and only if $\tau^{-1}\sigma \in Aut_{E(a)}(F)$,[4] so that there are k distinct cosets.

Lemma 33.8: If F is a finite field extension of E, the following properties are equivalent:

a) F is a Galois extension of E.

b) F is a normal and separable extension of E.

c) F is a splitting field extension for some $P \in E[x]$, with P separable over E.

Proof: a) implies b). Let F be a Galois extension of E, and $a \in F$, with minimal (monic irreducible) polynomial $P_a \in E[x]$. Let k be the size of the orbit of a under the action of $Aut_E(F)$, let ℓ be the number of distinct roots of P_a in F, so that, by Lemma 33.7, $|Aut_E(F)| = k\,|Aut_{E(a)}(F)|$. Because F is a Galois extension, $|Aut_E(F)| = [F:E]$, but since $|Aut_{E(a)}(F)| \le [F:E(a)]$, one deduces from $[F:E] = [F:E(a)]\,[E(a):E]$ that $[F:E(a)]\,[E(a):E] = [F:E] = |Aut_E(F)| = k\,|Aut_{E(a)}(F)| \le k\,[F:E(a)]$, hence $[E(a):E] \le k$. However, one has $k \le \ell \le deg(P_a) = [E(a):E]$ by Lemma 33.7, and one deduces then that $k = \ell = deg(P_a)$. That $\ell = deg(P_a)$ implies that P_a splits over F; this shows that F is a normal extension of E (since all the P_a for $a \in F$ split over F). That $k = deg(P_a)$ implies that the roots of P_a are distinct (they are the $\sigma(a)$ for $\sigma \in Aut_E(F)$), so that P_a is separable; this shows that F is a separable extension of E (since all the P_a for $a \in F$ have simple roots in F).

b) implies c). Let F be a normal and separable extension of E. Choose $a_1, \ldots, a_m \in F$ so that $F = E(a_1, \ldots, a_m)$ (for example, one may take a basis of F as an E-vector space), and let $f = \prod_{i=1}^m P_{a_i} \in E[x]$. Each P_{a_i} is irreducible by definition, and separable since F is a separable extension of E, so that f is separable (Definition 33.5). Each P_{a_i} splits over F, since F is a normal extension of E, and the roots of f contain all the a_i, which with E generate $E(a_1, \ldots, a_m) = F$, so that F is a splitting field extension for f over E.

c) implies a). Let F be a splitting field extension for a separable $f \in E[x]$. One establishes the result by induction on $[F:E]$ (simultaneously for all E, F, f) that $|Aut_E(F)| = [F:E]$, so that F is a Galois extension of E.

If $[F:E] = 1$, one has $F = E$, and there is nothing to prove, so one assumes that $n = [F:E] > 1$. Let $a \in F \setminus E$ with $f(a) = 0$,[5] so that its monic irreducible polynomial $P_a \in E[x]$ is an irreducible factor of f, which is then separable by Definition 33.5; since F is a splitting field extension, it is a normal field extension of E, so that P_a splits over F, and because F is a separable field extension of E, it has $k = deg(P_a) = [E(a):E]$ distinct roots in F. Let $a_1, \ldots, a_k$ be these roots, so that for each i, f is separable over $E(a_i)$ by Lemma 33.6, and F is a splitting field extension for f over $E(a_i)$.[6] Also $[F:E(a_i)] = \frac{n}{k}$ by Lemma 33.7, which is $< n$ since $k > 1$ (because $a \notin E$), and by the induction hypothesis $|Aut_{E(a_i)}(F)| = \frac{n}{k}$. For each i, there is a unique isomorphism σ_i from $E(a)$ onto $E(a_i)$ extending id_E on E, and $\sigma_i(a) = a_i$. By the uniqueness of splitting field extension up to isomorphism, σ_i can be extended (not in a unique way) to an automorphism ρ_i of F. For $i \in \{1, \ldots, k\}$ and $\sigma \in Aut_{E(a_i)}(F)$, one considers the automorphism $\sigma \circ \rho_i \in Aut(F)$; for a given i, this creates $\frac{n}{k}$ distinct elements of $Aut_E(F)$, and since $\sigma \circ \rho_i(a) = a_i$ one has $\sigma \circ \rho_i \ne \tau \circ \rho_j$ if $i \ne j$ and $\tau \in Aut_{E(a_j)}(F)$, so that one has $\frac{n}{k}\,k = n$ distinct elements of $Aut_E(F)$, i.e. $|Aut_E(F)| \ge n$, but one has $|Aut_E(F)| \le [F:E] = n$.

[4] If $\chi \in Aut_E(F)$, then χ fixes $E(a)$ if and only if $\chi(a) = a$. It is necessary that $a \in E(a)$ be fixed by χ, and then it is sufficient, since it implies $\chi(a^n) = a^n$ for all $n \in \mathbb{Z}$, and one has $E(a) = E[a]$, because a is algebraic over E (since $[F:E] < \infty$).

[5] Such an a exists since F is generated by the roots of f, which are not all in E, since $F \ne E$.

[6] Because F is a field extension of $E(a_i)$, f splits in F, and the smallest field containing $E(a_i)$ and the roots of f contains E and the roots of f, so that it is F.