## 1. The Main Fact of Galois Theory.

*(following Artin)*

If $K$ is a field and $X$ a set, we shall denote by $\mathrm{Map}(X, K)$ the $K$ -space of functions from $X$ to $K$. The group of automorphisms of $K$ fixing a subfield $k \subset K$ will be labeled $\mathrm{Aut}_k(K)$; if $k$ is the prime field, the subscript will be omitted.

We start with a lemma due to Dedekind.

LEMMA 1.1: $\mathrm{Aut}(K)$ is a $K$-independent subset of $\mathrm{Map}(K, K)$.

*Proof:* Assuming the contrary, consider a shortest (i.e. with the fewest terms) non-trivial linear relation

$$x_1\sigma_1(\alpha) + \cdots + x_r\sigma_r(\alpha) = 0, \tag{1}$$

for all $\alpha \in K$, with $\sigma_j \in \mathrm{Aut}(K)$. Choose $\beta \in K$ such that $\sigma_1(\beta) \neq \sigma_r(\beta)$, and modify (1) in two ways: first substitute $\beta\alpha$ for $\alpha$, and secondly just multiply by $\sigma_1(\beta)$. Subtracting the two equations so obtained, we get a new relation whose coefficients are $y_j = x_j(\sigma_j(\beta) - \sigma_1(\beta))$. Since $y_1 = 0$ and $y_r \neq 0$, it is shorter than (1).

*Definitions:* If $G$ is a subgroup of $\mathrm{Aut}(K)$, the *fix -field* $K^G$ of $G$ is the set of all $\alpha \in K$ such that $\sigma(\alpha) = \alpha$ for all $\sigma \in G$. For given $G$, every $\alpha \in K$ has a *canonical image* in $\mathrm{Map}(G, K)$, namely the map $\sigma \mapsto \sigma(\alpha)$. The canonical image defines a $K^G$- homomorphism $K \to \mathrm{Map}(G, K)$

LEMMA 1.2: If $S \subset K$ is $K^G$-independent, then the canonical image of $S$ in $\mathrm{Map}(G, K)$ is $K$-independent.

*Proof:* Again consider a shortest non-trivial linear relation

$$x_1\sigma(\alpha_1) + \cdots + x_r\sigma(\alpha_r) = 0, \tag{2}$$

for all $\sigma \in G$, with $\alpha_i \in S$. We may assume that $x_1 = 1$. Moreover, we note that not all $x_i$ are in $K^G$, otherwise we get a contradiction to linear independence, when we set $\sigma =$ identity in (2). Say, $x_r \notin K^G$. Now choose $\tau \in G$ such that $\tau(x_r) \neq x_r$, and modify (2) in two ways: first substitute $\tau\sigma$ for $\sigma$, and secondly apply $\tau$ to both sides. Subtracting the two equations so obtained, we get a new relation whose coefficients are $y_i = x_i - \tau(x_i)$. Since $y_1 = 0$ and $y_r \neq 0$, it is shorter than (2).

THEOREM 1.3: Let $G \subset \mathrm{Aut}(K)$ be a subgroup, and put $k = K^G$. Then

$$\dim_k K = |G| \qquad \text{and} \qquad G = \mathrm{Aut}_k(K),$$

unless both $\dim_k K$ and $|G|$ are infinite.

*Proof:* Let $T = \{\sigma_1, \ldots, \sigma_n\} \subset G$ and $S = \{\alpha_1, \ldots, \alpha_m\} \subset K$ be finite subsets. Let $A_{S,T}$ be the $m \times n$ matrix whose $i, j$-th entry is $\sigma_j(\alpha_i)$.

If $|G| < \infty$ take $T = G$. Then, by Lemma 2, the rows of $A_{S,T}$ are $K$-independent whenever $S$ is $k$-independent. Hence $\dim_k K \leq n = |G|$.

If $\dim_k K < \infty$, take $S$ to be a basis of $K$ over $k$. Then, by Lemma 1, the columns of $A_{S,T}$ are independent, for any $T$. Hence $|G| \leq m = \dim_k K$.

The full automorphism group $\mathrm{Aut}_k(K)$ could not be larger than $G$ without driving up $\dim_k K$.

REMARK 1.4: For an *arbitrary* pair of fields $K \supset k$, the theorem says only:

$$|\mathrm{Aut}_k(K)| \ \leq \ \dim_k K, \tag{3}$$

since $k$ may be *smaller* than the fix-field of $\mathrm{Aut}_k(K)$.

If $|\mathrm{Aut}_k(K)| = \dim_k K$, the extension $K/k$ is called a *Galois extension*, and its automorphism group is also known as its *Galois group*. In such a situation, the lock-step agreement between group orders and field dimensions (given by the theorem) yields an *injection* $H \mapsto K^H$ of the set of subgroups of $G$ into the set of intermediate fields $k = K^G \subset K^H \subset K = K^{\{1\}}$. Later we shall prove this to be *bijective.*

## 2. Finite Field Extensions.

Fields have two virtues which greatly facilitate the study of their extensions.

Firstly, if $E \supset K$ are fields, $E$ is a $K$-space whose dimension (also called *degree*) is denoted by $[E : K]$. If this is $< \infty$ we say that $E/K$ is a *finite field extension*. We have

$$F \supset E \supset K \qquad \Longrightarrow \qquad [F : K] = [F : E] \cdot [E : K],$$

because a $K$-basis of $F$ can be obtained by pairwise multiplication of an $E$-basis of $F$ with a $K$-basis of $E$.

Secondly, the polynomial ring $R = K[X]$ over a field $K$ is a principal domain. This implies that any finite extension $E/K$ can be built up by adjoining roots of polynomials. Indeed, any $(\alpha) \in E$ yields an epimorphism $K[X] \to K[\alpha] \subset K(\alpha)$ whose kernel must be prime, hence maximal. Therefore $K[\alpha] \cong K[X]/(p(X))$ *is* a field, hence $= K(\alpha)$, and $[K(\alpha) : K] = \deg p(X)$. The ideal $(p)$ is uniquely determined by $\alpha$ and $K$; its lone monic inhabitant is known as the *minimal polynomial* of $\alpha$ over $K$. Given another $\beta \in E$, we can repeat the process: $K[\alpha, \beta] = K(\alpha)[\beta] = K(\alpha, \beta)$, and inductively

$$K[\alpha_1, \ldots, \alpha_r] = K(\alpha_1, \ldots, \alpha_r),$$

for any $\alpha_1, \ldots, \alpha_r$ in $E$. Since $E$ has a finite basis over $K$, it must itself be of that form.

If $E = K(\alpha_1, \ldots, \alpha_n)$ where the polynomial $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$ has coefficients in $K$, then $E$ is called a *splitting field* for $f(X)$, and $[E : K] \leq n!$. To see this inequality, note that $\deg f(X) = n$ implies $[K(\alpha_1) : K] \leq n$. In $K(\alpha_1)$, however, there is a partial factorization $f(X) = (X - \alpha_1)g(X)$, with $\deg g(X) = n - 1$, and by induction hypothesis $[E : K(\alpha_1)] \leq (n-1)!$.

We shall later see that splitting fields are unique up to isomorphism. For the moment, we concentrate on their existence.

Indeed, if $p \in R$ is irreducible, the ideal $(p)$ is maximal, and $R/(p) = K[\xi]$ is a field generated by the coset $\xi = X + (p(X))$, with $p(\xi) = 0$. Therefore, if $f(X) \in R$ has degree $n$, and we use an irreducible factor $p$ of $f$ to construct $L = K[\xi]$, then $[L : K] \leq n$. Since $f(X) = (X - \xi)g(X)$ with $g(X) \in L[X]$ of degree $n - 1$, induction yields a field $F$ in which $g(X)$, and hence $f(X)$, splits into linear factors, and which is generated by the roots of $f(X)$. Let us summarize.

THEOREM 2.1: Let $E/K$ be a finite field extension, and put $R = K[X]$. Then

(a) If $\alpha_1, \ldots, \alpha_r \in E$, then $K[\alpha_1, \ldots, \alpha_r]$ is a field.
(b) For every $\alpha \in E$, the map $X \mapsto \alpha$ yields an isomorphism $R/(p) \to K[\alpha]$, where $p(X)$ is the minimal polynomial of $\alpha$ over $K$.
(c) Every $f \in R$ has a splitting field $E$; if $\deg f = n$, then $[E : K] \leq n!$.

REMARK 2.2: Certain algebraic (and geometric) algorithms can be interpreted as the step-wise construction of a finite field extension. Take the classical ruler-and-compass problems. One is given a set of points (coordinates) and tries to create more points by intersecting lines and/or circles obtained from the existing ones. Since one is thus geometrically solving equations which are at most quadratic, the evolving extension field will have 2-power degree. It is easy to see that doubling the cube or trisecting an angle necessarily involve extensions of degree 3. Therefore these are unattainable.

Another famous problem, solving polynomial equations by radicals, cannot be decided by degree alone. Solution by radicals means by an algorithm in which each step involves only rational operations and equations of the type $X^n - s = 0$.

*Definition:* $F/K$ is called a *simple radical extension* if $F = K[\alpha]$ with $\alpha^n \in K$ for some $n$ (which need not be $= [F : K]$). $E/K$ is said to be *constructible by radicals*, if it is obtainable by a finite sequence $K = L_0 \subset L_1 \subset \cdots \subset L_m = E$ of simple radical extensions $L_i/L_{i-1}$.

One of the original aims of Galois theory was to find a criterion for deciding whether the roots (i.e. splitting field) of a given polynomial were so constructible.

## 3. Cyclic Field Extensions.

A field extension $K/k$ is called *cyclic of degree* $n$, if it is a Galois extension with $\mathrm{Gal}(K/k)$ cyclic of order $n$. As an exercise in Galois theory, we shall characterize such extensions for the case of a sufficiently rich ground field $k$ — by which we mean that $k$ should contain $n$ different roots of $X^n - 1$, the so-called $n$-th roots of unity. We start with a lemma about these.

LEMMA 3.1: In any field, the roots of $X^n - 1$ form a cyclic multiplicative group of order $\leq n$.

*Proof:* The set $W$ of these roots has $\leq n$ elements. It is a multiplicative group since $a^n = 1$ and $b^n = 1$ implies $(ab)^n = 1$. By the theorem on finitely generated $\mathbf{Z}$-modules, $W$ has a subgroup $C$ which is cyclic of order $d$, where $w^d = 1$ for all $w \in W$. Since $X^d - 1$ can have only $d$ roots, $W$ must fit into $C$.

*Definition:* An $n$-th root of unity is *primitive* if its powers form a group of order $n$.

THEOREM 3.2: Let $K \supset k$ be fields, with $k$ containing a primitive $n$th root of unity.

Then $K/k$ is cyclic of degree $n$ if and only if $K = k(\theta)$ with $\theta^n \in k$ and no smaller power of $\theta$ in $k$.

*Proof:* Consider first an arbitrary field $F = k(t)$ such that $t^n = s \in k$, with $n$ minimal, and look at the polynomial

$$f(X) = X^n - s = \prod_{w \in W_n} (X - wt),$$

where $W_n$ denotes the roots of $X^n - 1$. If $p(X)$ is a prime divisor of $f(X)$ in $k[X]$, say the product of $m$ of the factors $X - wt$, its constant term would be $\pm ut^m$, with some $u \in W_n \subset k$, and we would get $t^m \in k$. Since $n$ is minimal, we conclude that $f(X)$ is irreducible, and the obvious ring surjection $k[X]/(f(X)) \to k[t] = F$ is an isomorphism of fields. In particular, the automorphisms of $k[X]/(f(X))$ given by $X \mapsto wX$, with $w \in W_n$, translate faithfully into elements of $\mathrm{Aut}_k(F)$, where they form a cyclic group $G$ of order $n$. By Galois theory, $[F : F^G] = n$; but $[F : k] = n$ as well and hence $F^G = k$. Therefore $F/k$ is cyclic of degree $n$.

Conversely, let $K/k$ be cyclic with group $G$ of order $n$, and choose an isomorphism $\zeta : G \to W_n$. For any $\alpha \in K$ consider the *Lagrange resolvent*

$$\theta(\zeta, \alpha) = \sum_{\sigma \in G} \zeta(\sigma^{-1})\sigma(\alpha),$$

whose purpose in life is to satisfy the marvellous functional equation (for all $\tau \in G$)

$$\tau(\theta(\zeta, \alpha)) = \sum_{\sigma \in G} \zeta(\sigma^{-1})\tau\sigma(\alpha) = \zeta(\tau) \sum_{\rho \in G} \zeta(\rho^{-1})\rho(\alpha) = \zeta(\tau)\theta(\zeta, \alpha),$$

obtained by the change of variable $\rho = \tau\sigma$. By Dedekind's Lemma, $\theta(\zeta, \alpha) = \theta \neq 0$, for suitable $\alpha$. Then $\tau(\theta)/\theta = \zeta(\tau)$ for all $\tau \in G$, and more generally $\tau(\theta^m)/\theta^m = \zeta(\tau)^m$.This shows that $\theta^m$ is fixed by $G$, hence lies in $k$, if and only if $\zeta(\tau)^m = 1$ for all $\tau$. Therefore $\theta^n \in k$, and $n$ is minimal. By the first part of this proof, $[k(\theta) : k] = n$. Therefore $K = k(\theta)$, as was to be shown.

*Example:* For a different kind of cyclic extension, let $k$ denote the rationals, and consider $K = k(\epsilon)$, where $\epsilon = e^{2\pi i/p}$ is a complex $p$-th root of unity, $p > 2$ a prime. Then $\epsilon$ is a root of $f(X) = X^{p-1} + \cdots + X + 1 = (X^p - 1)(X - 1)^{-1}$, which is irreducible over $k$ by Eisenstein's criterion applied to $f(Y + 1) = ((Y + 1)^p - 1)Y^{-1}$. Hence, for any non-zero $u \in \mathbf{Z}/(p)$ , we get a legitimate automorphism $\sigma_u : \epsilon \mapsto \epsilon^u$ of $K/k$, which is the identity only if $u = 1$.

Thus $u \mapsto \sigma_u$ constitutes an injection of the full multiplicative group $U_p$ of $\mathbf{Z}/(p)$ into $\mathrm{Aut}_k(K)$. By Lemma 3.1, $U_p$ is cyclic of order $p - 1$. Since $[K : k] = p - 1$, this means that the fix-field is precisely $k$, and $K/k$ is cyclic. However, for $p > 3$ it is not generated by any $(p - 1)$-st root of anything.

## 4. Solvability.

If $K/k$ is a Galois extension with group $G$ and $H \subset G$ is a subgroup with fix-field $F = K^H$, then obviously $K/F$ is a Galois extension with group $H$.

But if $H$ is a *normal* subgroup, $F$ is moreover $G$- invariant (since $h(gx) = gx \iff g^{-1}hg(x) = x$), and we get a natural group-homomorphism

$$\mathrm{res}_{K|F} : \mathrm{Aut}_k(K) \longrightarrow \mathrm{Aut}_k(F),$$

by restriction to $F$. Conversely, consider *any* subextension $F/k \subset K/k$ invariant under $G$. Then a restriction map can be defined as above, and its kernel is the (normal) subgroup $H \subset G$ which fixes $F$. The injection $G/H \hookrightarrow \mathrm{Aut}_k(K)$ gives the first of the following three inequalities

$$[G : H] \leq |\mathrm{Aut}_k(F)| \leq [F : k] \leq [K^H : k],$$

whose outer terms are equal, making $F = K^H$, and $F/k$ a Galois extension with $\mathrm{Aut}_k(F) \cong G/H$. Let us summarize.

LEMMA 4.1: Let $K/k$ a Galois extension with group $G$, and consider a subextension $k \subset F \subset K$.
Then $F$ is $G$- invariant if and only if $F = K^H$, for some normal subgroup $H \lhd G$.
In that case, $F/k$ is Galois with group $\cong G/H$.

The following result is immediate from this lemma and the theorem on cyclic extensions.

THEOREM 4.2: Let $K/k$ be Galois with group $G$, and $k$ containing a primitive $n$-th root of unity.
Then $K/k$ is constructible by radicals if and only if $G$ is solvable.

*Proof:* If $G$ is solvable, it has a solvable normal subgroup $H$ such that $G/H$ is cyclic. By the Lemma, $K^H/k$ is cyclic, hence radical. $K/K^H$ is Galois with group $H$, hence constructible by radicals according to the induction hypothesis.

If $F = k(\theta)$ is the first link in a chain of radical extensions leading to $K$, then it is $G$-invariant, because $\sigma(\theta)\theta^{-1}$ is an $n$-th root of unity, hence $\sigma(\theta) \in F$, for all $\sigma \in G$. By the Lemma, $F = K^H$ with $H$ normal, and $G/H \cong \mathrm{Aut}_k(F)$, hence cyclic. The induction hypothesis applied to $K/F$ says that $H$ is solvable.

THEOREM 4.3: Let $L = k(t_1, \ldots, t_n)$ be the field of rational functions in $n$ indeterminates, and $K = k(s_1, \ldots, s_n)$ the subfield generated by the elementary symmetric functions $s_1, \ldots, s_n$.

(a) $L/K$ is Galois with group $G = \mathcal{S}_n$.
(b) If $k$ is of characteristic 0, and $n \geq 5$, the extension $L/K$ is not constructible by radicals.

*Proof:* $G$ acts on $L$ by permuting the indeterminates. Obviously $K \subset L^G$. But $L$ is a splitting field of the polynomial $\prod_i (X - t_i)$, whose coefficients *are* the $s_i$. Hence $[L : K] \leq n!$. On the other hand $[L : L^G] = n!$, and therefore $L^G = K$.

For (b), we may assume that $k$ contains all kinds of roots of unity. (Otherwise adjoin them to get bigger fields $k', K', L'$; if $L/K$ were constructible by radicals, so would $L'/K'$ be.)

By Theorem 4.2, $G$ would have to be solvable. But for $n \geq 5$, the group $\mathcal{A}_n$ of even permutations is *not* solvable. In fact, $\mathcal{A}_n$ (with $n \geq 5$) is generated by commutators, which are of course trivialized in any abelian factor group.

In fact, we can show that any 3-cycle (i.e. permutation with $n - 3$ fixed points) *is* a commutator. To get the 3-cycle $(ijk)$, take 2 further points $h, l$ (here we need $n \geq 5$) and define 3-cycles $\sigma, \tau$ involving $h, i, j$ and $j, k, l$, respectively; then $\sigma^{-1}\tau^{-1}\sigma\tau$ fixes everything except possibly $i, j, k$. Being even, it cannot fix just one of these; being non-trivial, it cannot fix more. Hence it is either $(ijk)$ or its inverse. Using similar reasoning, one easily convinces oneself that every non-trivial product of two transpositions is either a 3-cycle or a product of two. Therefore $\mathcal{A}_n$ is generated by commutators.

This proves what is known as the Insolubility of the Quintic.

## 5. Normality.

Since fields have no ideals, all non-trivial ring homomorphisms $E \to F$ are injective. They will be referred to as *embeddings*. Even if we are ultimately interested in automorphisms, it behooves us to consider embeddings, because this more general notion is better adapted to inductive constructions.

LEMMA 5.1: Let $E/K$ be a finite extension, $\sigma : K \to L$ an embedding. Then there exists a finite extension $F/L$ and an embedding $\tau : E \to F$ compatible with $\sigma$.

*Proof:* Induction on $[E : K]$. Let $\alpha \in E$ be such that $K(\alpha) \cong K[X]/(p(X))$ for some irreducible $p$ of degree $> 1$; let $p^\sigma(X) \in L[X]$ be its $\sigma$-image, and $q(X)$ be an irreducible factor of same. Then $\sigma$ induces an embedding of fields $K(\alpha) \cong K[X]/(p(X)) \to L[X]/(q(X))$. Since $[E : K(\alpha)] < [E : K]$, induction does it.

REMARK 5.2: This is easily generalized to a finite set $\sigma_i : K \to L$ giving rise to extensions $\tau_i : E \to F$, with a single $F$. We apply the lemma once, getting $\tau_1$ and $F_1$, then regard the remaining $\sigma_i$ as embeddings into $F_1$, extendable by induction hypothesis.

*Definition:* A finite field extension $E/K$ is *normal* if every $F/K$ has at most one subextension isomorphic to $E/K$.

THEOREM 5.3: For a finite field extension $E/K$ the following properties are equivalent.

(i) If an irreducible $K$-polynomial has a root in $E$, then it splits in $E$.
(ii) $E/K$ is the splitting field of some $K$- polynomial.
(iii) $E/K$ is normal.

*Proof:* (i) $\Rightarrow$ (ii): (i) says that $E/K$ is a union of splitting fields, since every $\alpha \in E$ is at once accompanied all its brothers and sisters. Being of finite degree, it must be a *finite* union of splitting fields, say of $f_1(X), \ldots, f_s(X) \in K[X]$, but then it is a splitting field for the product of these.

(ii) $\Rightarrow$ (iii): Let $E/K$ be a splitting field of $f(X) \in K[X]$. If $\tau : E \to F$ is an embedding, it changes the splitting of $f(X) \in E[X]$ to one of $f(X) \in F[X]$. But the linear factors, say $\{X - \beta_j\}$, of the latter do not depend on $\tau$ (unique factoring in $F[X]$), and the $\tau$-image of $E$ is the field $K(\{\beta_j\}) \subset F$.

(iii) $\Rightarrow$ (i): Let $f(X)$ be the irreducible polynomial for $\alpha \in E$, and let $L$ be a splitting field for $f(X)$, say $f(X) = (X - \beta_1) \cdots (X - \beta_r)$ in $L$. Let $\sigma_i : \alpha \mapsto \beta_i$ be the corresponding embedding of $K(\alpha) \to L$. By Remark 1, there exists an $F/K$ admitting extensions $\tau_i : E \to F$. By (iii), there is a unique $E' \subset F$ such that $\tau_i(E) = E'$ for all $i$. Since $\beta_i \in \tau_i(E)$ by construction, $f(X)$ splits in $E'$, hence in $E$.

REMARK 5.4: (a) If $E/K$ and $E'/K$ are splitting fields of the same $f(X)$, they are isomorphic. Indeed, Lemma 5.1 extends the inclusion $K \to E'$ to an embedding $\tau : E \to F$ with $F \supset E'$, but $\tau(E) = E'$ since both are generated by the roots of $f$.

(b) Every finite $E/K$ can be embedded in a *normal* $F/K$, for instance into the splitting field of a polynomial that kills all its generators.

(c) If $E/K$ is a normal subextension of a Galois extension $L/K$, it is invariant under the Galois group (as $\sigma(E) = E$ by normality). Hence Lemma 4.1 implies that $H \mapsto L^H$ is a bijection between normal subgroups of $G$ and normal subextensions of $E/K$.

*Example:* This might be the right place to tell the story of finite fields. In such a field $K$ the subfield generated by 1 must be $k = \mathbf{Z}/(p)$, for some natural prime $p$. If $[K : k] = n$, the number of elements in $K$ is evidently $q = p^n$. By Lemma 4.1, the multiplicative group of $K$ is cyclic of order $q - 1$; hence $0 \neq u \in K \Rightarrow u^{q-1} = 1$. Hence $K$ consists precisely of the $q$ roots of $X^q - X$, and is the splitting field of this polynomial.

The Galois theory of finite fields is pleasantly simple. With $K$ as above, let $\phi : K \to K$ be given by $\phi : x \mapsto x^p$. Being a ring endomorphism with trivial kernel, it is an automorphism. Being a permutation of a finite set, it has finite order, which by Galois matches the degree of $K$ over the fix-field $k$. Hence $K/k$ is cyclic, with its Galois group $G$ generated by $\phi$. Intermediate fields $k \subset F \subset K$ are exactly the fix-fields of subgroups of $G$: such $F$ has $p^m$ elements, if and only if it satisfies $\phi^m(x) = x^{p^m} = x$.

## 6. Separability.

A polynomial $f(X)$ over a field $K$ is *separable* if it has no multiple roots in any extension of $K$; i.e. if $f(\alpha) = 0$ implies $f'(\alpha) \neq 0$, where $f'$ denotes the derivative. For irreducible $f$ this is equivalent to saying that $f'(X) \neq 0$ — a condition that is sometimes violated at characteristic $p$ (e.g. if $f(X) = X^p - a$ ). Note that separability of a polynomial is independent of ground- field. An element of an extension $E/K$ is *separable* if it is the root of a separable polynomial, and $E/K$ is *separable* if all its elements are.

The following lemma shows what separability is good for: it allows measuring the degree of an extension in terms of availability of embeddings.

LEMMA 6.1: Let $F/L$ be normal and $\sigma : K \to L$ an embedding which is extendable to some $\tau : E \to F$, where $[E : K] = n < \infty$.

Then the number of such extensions is $\#\{\tau\} \leq n$, with equality if and only if $E/K$ is separable.

*Proof:* Let $\alpha \in E$ and $p(X)$ its minimal polynomial over $K$. If $p^\sigma(X) = (X - \beta_1) \cdots (X - \beta_m)$ in $F$, the only possible extensions of $\sigma$ are given by $\rho_i : \alpha \mapsto \beta_i$; hence there are $\leq m = [K(\alpha) : K]$ of them, with equality if and only if $\beta_1, \ldots, \beta_m$ are distinct, i.e. $p(X)$ is separable, i.e. $\alpha$ is separable. By induction, each of these $\rho_i$ extends to $\leq [E : K(\alpha)]$ embeddings $E \to F$, with equality if $E/K$, and hence $E/K(\alpha)$, is separable. Therefore the total number is $\leq [K(\alpha) : K] \cdot [E : K(\alpha)] = [E : K]$, with equality in the separable case. If $\alpha$ was *not* separable, the first stage of this count would have created an irreparable short-fall. Thus the maximality of $\#\{\tau\}$ forces every element of $E$ to be separable over $K$.

REMARK 6.2: The same proof shows: If $E = K(\alpha, \beta)$, with $\alpha$ separable over $K$, and $\beta$ separable over $K(\alpha)$, then $E/K$ is separable. In particular, the $K$-separable elements in an extension $L/K$ form a subfield.

Any finite separable $E/K$ can be embedded in a *normal* one, e.g. a splitting field of the the minimal polynomials of all its generators. This is important in view of the following result.

THEOREM 6.3: A finite extension $E/K$ is separable and normal, if and only if it is Galois, i.e. $|\mathrm{Aut}_K(E)| = [E : K]$.

*Proof:* Most of this is immediate from the Lemma, by taking $E/K = F/L$ and $\sigma =$ identity. Just note that self-embeddings, being degree preserving, are the same as automorphisms. To check that abundance of automorphisms implies normality, let $F/K$ be *any* extension and $\tau : E \to F$ be an embedding over $K$. Then $\{\tau \circ \rho\}$, as $\rho$ ranges over the $[E : K]$ available automorphisms, constitutes the sum total of *all* embeddings, and $F/K$ has only one subextension isomorphic to $E/K$.

REMARK 6.4: This theorem sets the stage for most applications of Galois theory.

(a) If $E \supset F \supset K$ and $E/K$ is Galois, then so is $E/F$ by our new criterion. Now $\mathrm{Aut}_F(E)$ is by definition that subgroup $H$ of $\mathrm{Aut}_K(E)$ which fixes $F$. Comparing degrees, we get $F = E^H$. Conclusion: $H \mapsto E^H$ defines a *bijection* between subgroups of $\mathrm{Aut}_K(E)$ and subextensions of $E/K$. (see also Remarks 1.4 and 5.4 (c)).

(b) Every finite separable $F/K$ is monogenic; i.e. $F = K[\theta]$ . For finite fields, we have seen this already: their multiplicative groups are cyclic. So we take $K$ to be infinite and show that $K[\alpha, \beta] = K[\gamma]$, for any $\alpha, \beta$ and suitable $\gamma$. Embedding $F$ into some $E$ which is Galois over $K$, we see that there are only finitely many fields $L$ such that $K \subset L \subset F$ (they correspond to subgroups of a finite group). Hence there are distinct $c_1, c_2 \in K$ such that $K[\alpha + c_1\beta] = K[\alpha + c_2\beta]$, and therefore $= K[\alpha, \beta]$.

(c) Here is an algebraic version of the Fundamental Theorem of Algebra: Let $L/K$ be a quadratic field extension of characteristic 0 such that (i) $L$ has no quadratic extensions, and (ii) $K$ has no extensions of odd degree $> 1$; then $L$ is algebraically closed. *Proof:* Any finite extension $F/L$ would be embeddable in a Galois extension $E/K$, say with Galois group $G$. Let $G_1$ be a Sylow 2-group and $K_1$ its fix-field. Since $[K_1 : K]$ is odd, (ii) says that $K_1 = K$, and hence $G = G_1$ is a 2-group. Now let $H$ be the Galois group of $E/L$. Being a subgroup of $G$, it too is a 2-group. If it were non-trivial, it would have a subgroup of index 2, corresponding to a quadratic extension of $K$, contradicting (i). Hence $E = L$, as was to be shown.