Galois Theory Quick Reference

Goal. Some polynomials cannot be "solved" using $+$, $-$, $\times$, $\div$ and $\sqrt[n]{\ }$.
Galois Theory. Roughly, there is a correspondence

{field extensions}	$\overset{\text{The Fundamental}}{\underset{\text{Theorem}}{\longleftrightarrow}}$	{groups}
{extensions by roots}	$\longrightarrow$	{"solvable groups"}
splitting field of $3x^5 - 15x + 5$	$\longrightarrow$	the non-solvable permutation group S_5

To do.

1. More on splitting fields.
2. Quick reminders on group theory.
3. Precise statement of the fundamental theorem.
4. Examples for the fundamental theorem.
5. On solvable groups: definition, basic properties, S_5 is not solvable.
6. "Extensions by radicals" correspond to solvable groups.
7. The splitting field of $3x^5 - 15x + 5$ corresponds to S_5.
8. Proof of the fundamental theorem.

Dror Bar-Natan: Classes: 2007-08: Math 401 Polynomials, Equations, Fields:

Galois Theory Quick Reference

Goal. Some polynomials cannot be "solved" using $+$, $-$, $\times$, $\div$ and $\sqrt[n]{\ }$.
Galois Theory. Roughly, there is a correspondence

{field extensions} The Fundamental Theorem {groups}
{extensions by roots} $\longrightarrow$ {"solvable groups"}
splitting field of $3x^5 - 15x + 5$ $\longrightarrow$ the non-solvable permutation group S_5

To do.

1. More on splitting fields.
2. Quick reminders on group theory.
3. Precise statement of the fundamental theorem.
4. Examples for the fundamental theorem.
5. On solvable groups: definition, basic properties, S_5 is not solvable.
6. "Extensions by radicals" correspond to solvable groups.
7. The splitting field of $3x^5 - 15x + 5$ corresponds to S_5.
8. Proof of the fundamental theorem.

Dror Bar-Natan: Classes: 2007-08: Math 401 Polynomials, Equations, Fields:

Galois Theory Quick Reference

Goal. Some polynomials cannot be "solved" using $+$, $-$, $\times$, $\div$ and $\sqrt[n]{\ }$.
Galois Theory. Roughly, there is a correspondence

{field extensions} The Fundamental Theorem {groups}
{extensions by roots} $\longrightarrow$ {"solvable groups"}
splitting field of $3x^5 - 15x + 5$ $\longrightarrow$ the non-solvable permutation group S_5

To do.

1. More on splitting fields.
2. Quick reminders on group theory.
3. Precise statement of the fundamental theorem.
4. Examples for the fundamental theorem.
5. On solvable groups: definition, basic properties, S_5 is not solvable.
6. "Extensions by radicals" correspond to solvable groups.
7. The splitting field of $3x^5 - 15x + 5$ corresponds to S_5.
8. Proof of the fundamental theorem.

Dror Bar-Natan: Classes: 2007-08: Math 401 Polynomials, Equations, Fields:

Galois Theory Quick Reference

Goal. Some polynomials cannot be "solved" using $+$, $-$, $\times$, $\div$ and $\sqrt[n]{\ }$.
Galois Theory. Roughly, there is a correspondence

{field extensions} The Fundamental Theorem {groups}
{extensions by roots} $\longrightarrow$ {"solvable groups"}
splitting field of $3x^5 - 15x + 5$ $\longrightarrow$ the non-solvable permutation group S_5

To do.

1. More on splitting fields.
2. Quick reminders on group theory.
3. Precise statement of the fundamental theorem.
4. Examples for the fundamental theorem.
5. On solvable groups: definition, basic properties, S_5 is not solvable.
6. "Extensions by radicals" correspond to solvable groups.
7. The splitting field of $3x^5 - 15x + 5$ corresponds to S_5.
8. Proof of the fundamental theorem.

The Fundamental Theorem of Galois Theory. Let F be a field of characteristic 0 and let E be a splitting field over F. Then there is a bijective correspondence between the set $\{K : E/K/F\}$ of intermediate field extensions K lying between F and E and the set $\{H : H < \mathrm{Gal}(E/F)\}$ of subgroups H of the Galois group $\mathrm{Gal}(E/F)$ of the original extension E/F:

$$\{K : E/K/F\} \quad \leftrightarrow \quad \{H : H < \mathrm{Gal}(E/F)\}.$$

The bijection is given by mapping every intermediate extension K to the subgroup $\mathrm{Gal}(E/K)$ of elements in $\mathrm{Gal}(E/F)$ that preserve K,

$$\Phi : \; K \mapsto \mathrm{Gal}(E/K) := \{g : E \to E : g|_K = I\},$$

and reversely, by mapping every subgroup H of $\mathrm{Gal}(E/F)$ to its fixed field E_H:

$$\Psi : \; H \mapsto E_H := \{x \in E : \forall h \in H, \; hx = x\}.$$

This correspondence has the following further properties:

- It is inclusion-reversing: if $H_1 \subset H_2$ then $E_{H_1} \supset E_{H_2}$ and if $K_1 \subset K_2$ then $\mathrm{Gal}(E/K_1) > \mathrm{Gal}(E/K_2)$.
- It is degree/index respecting: $[E : K] = |\mathrm{Gal}(E/K)|$ and $[K : F] = [\mathrm{Gal}(E/F) : \mathrm{Gal}(E/K)]$.
- Splitting fields correspond to normal subgroups: If K in $E/K/F$ is the splitting field of a polynomial in $F[x]$ then $\mathrm{Gal}(E/K)$ is normal in $\mathrm{Gal}(E/F)$ and $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F)/\mathrm{Gal}(E/K)$.

The Fundamental Theorem of Galois Theory. Let F be a field of characteristic 0 and let E be a splitting field over F. Then there is a bijective correspondence between the set $\{K : E/K/F\}$ of intermediate field extensions K lying between F and E and the set $\{H : H < \mathrm{Gal}(E/F)\}$ of subgroups H of the Galois group $\mathrm{Gal}(E/F)$ of the original extension E/F:

$$\{K : E/K/F\} \quad \leftrightarrow \quad \{H : H < \mathrm{Gal}(E/F)\}.$$

The bijection is given by mapping every intermediate extension K to the subgroup $\mathrm{Gal}(E/K)$ of elements in $\mathrm{Gal}(E/F)$ that preserve K,

$$\Phi : \; K \mapsto \mathrm{Gal}(E/K) := \{g : E \to E : g|_K = I\},$$

and reversely, by mapping every subgroup H of $\mathrm{Gal}(E/F)$ to its fixed field E_H:

$$\Psi : \; H \mapsto E_H := \{x \in E : \forall h \in H, \; hx = x\}.$$

This correspondence has the following further properties:

- It is inclusion-reversing: if $H_1 \subset H_2$ then $E_{H_1} \supset E_{H_2}$ and if $K_1 \subset K_2$ then $\mathrm{Gal}(E/K_1) > \mathrm{Gal}(E/K_2)$.
- It is degree/index respecting: $[E : K] = |\mathrm{Gal}(E/K)|$ and $[K : F] = [\mathrm{Gal}(E/F) : \mathrm{Gal}(E/K)]$.
- Splitting fields correspond to normal subgroups: If K in $E/K/F$ is the splitting field of a polynomial in $F[x]$ then $\mathrm{Gal}(E/K)$ is normal in $\mathrm{Gal}(E/F)$ and $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F)/\mathrm{Gal}(E/K)$.

The Fundamental Theorem of Galois Theory. Let F be a field of characteristic 0 and let E be a splitting field over F. Then there is a bijective correspondence between the set $\{K : E/K/F\}$ of intermediate field extensions K lying between F and E and the set $\{H : H < \mathrm{Gal}(E/F)\}$ of subgroups H of the Galois group $\mathrm{Gal}(E/F)$ of the original extension E/F:

$$\{K : E/K/F\} \quad \leftrightarrow \quad \{H : H < \mathrm{Gal}(E/F)\}.$$

The bijection is given by mapping every intermediate extension K to the subgroup $\mathrm{Gal}(E/K)$ of elements in $\mathrm{Gal}(E/F)$ that preserve K,

$$\Phi : \; K \mapsto \mathrm{Gal}(E/K) := \{g : E \to E : g|_K = I\},$$

and reversely, by mapping every subgroup H of $\mathrm{Gal}(E/F)$ to its fixed field E_H:

$$\Psi : \; H \mapsto E_H := \{x \in E : \forall h \in H, \; hx = x\}.$$

This correspondence has the following further properties:

- It is inclusion-reversing: if $H_1 \subset H_2$ then $E_{H_1} \supset E_{H_2}$ and if $K_1 \subset K_2$ then $\mathrm{Gal}(E/K_1) > \mathrm{Gal}(E/K_2)$.
- It is degree/index respecting: $[E : K] = |\mathrm{Gal}(E/K)|$ and $[K : F] = [\mathrm{Gal}(E/F) : \mathrm{Gal}(E/K)]$.
- Splitting fields correspond to normal subgroups: If K in $E/K/F$ is the splitting field of a polynomial in $F[x]$ then $\mathrm{Gal}(E/K)$ is normal in $\mathrm{Gal}(E/F)$ and $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F)/\mathrm{Gal}(E/K)$.

The Fundamental Theorem of Galois Theory. Let F be a field of characteristic 0 and let E be a splitting field over F. Then there is a bijective correspondence between the set $\{K : E/K/F\}$ of intermediate field extensions K lying between F and E and the set $\{H : H < \mathrm{Gal}(E/F)\}$ of subgroups H of the Galois group $\mathrm{Gal}(E/F)$ of the original extension E/F:

$$\{K : E/K/F\} \quad \leftrightarrow \quad \{H : H < \mathrm{Gal}(E/F)\}.$$

The bijection is given by mapping every intermediate extension K to the subgroup $\mathrm{Gal}(E/K)$ of elements in $\mathrm{Gal}(E/F)$ that preserve K,

$$\Phi : \; K \mapsto \mathrm{Gal}(E/K) := \{g : E \to E : g|_K = I\},$$

and reversely, by mapping every subgroup H of $\mathrm{Gal}(E/F)$ to its fixed field E_H:

$$\Psi : \; H \mapsto E_H := \{x \in E : \forall h \in H, \; hx = x\}.$$

This correspondence has the following further properties:

- It is inclusion-reversing: if $H_1 \subset H_2$ then $E_{H_1} \supset E_{H_2}$ and if $K_1 \subset K_2$ then $\mathrm{Gal}(E/K_1) > \mathrm{Gal}(E/K_2)$.
- It is degree/index respecting: $[E : K] = |\mathrm{Gal}(E/K)|$ and $[K : F] = [\mathrm{Gal}(E/F) : \mathrm{Gal}(E/K)]$.
- Splitting fields correspond to normal subgroups: If K in $E/K/F$ is the splitting field of a polynomial in $F[x]$ then $\mathrm{Gal}(E/K)$ is normal in $\mathrm{Gal}(E/F)$ and $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F)/\mathrm{Gal}(E/K)$.

08-401/The Fundamental Theorem

From Drorbn

The statement appearing here, which is a weak version of the full **fundamental theorem of Galois theory**, is taken from Gallian's book and is meant to match our discussion in class. The proof is taken from Hungerford's book, except modified to fit our notations and conventions and simplified as per our weakened requirements.

Here and everywhere below our base field F will be a field of characteristic 0.

08-401/Navigation Panel [Hide]

#	Week of...	Links
1	Jan 9	About, Notes, HW1
2	Jan 16	HW2, Notes
3	Jan 23	HW3, Photo, Notes
4	Jan 30	HW4, Notes
5	Feb 6	HW5, Notes
6	Feb 13	On TT, Notes
R	Feb 20	Reading week
7	Feb 27	Term Test (and solution)
8	Mar 5	HW6, Notes
9	Mar 12	HW7, Notes
10	Mar 19	HW8, Notes, RC (PDF)
11	Mar 26	HW9, Notes
12	Apr 2	FT, HW10, Notes
13	Apr 9	Notes
S	Apr 14-25	Study Period: blackboards (http://katlas.math.toronto.edu/drorbn/bbs/show?shot=08401-080425-142418.jpg)
F	Apr 28	Final

Add your name / see who's in!

Register of Good Deeds

Contents

Statement

Theorem. Let E be a splitting field over F. Then there is a bijective correspondence between the set $\{K:E/K/F\}$ of intermediate field extensions K lying between F and E and the set $\{H:H<\operatorname{Gal}(E/F)\}$ of subgroups H of the Galois group $\operatorname{Gal}(E/F)$ of the original extension E/F:

$$\{K:E/K/F\} \quad \leftrightarrow \quad \{H:H<\operatorname{Gal}(E/F)\}.$$

The bijection is given by mapping every intermediate extension K to the subgroup $\operatorname{Gal}(E/K)$ of elements in $\operatorname{Gal}(E/F)$ that preserve K,

$$\Phi: \quad K\mapsto \operatorname{Gal}(E/K) := \{\phi:E\to E : \phi|_K = I\},$$

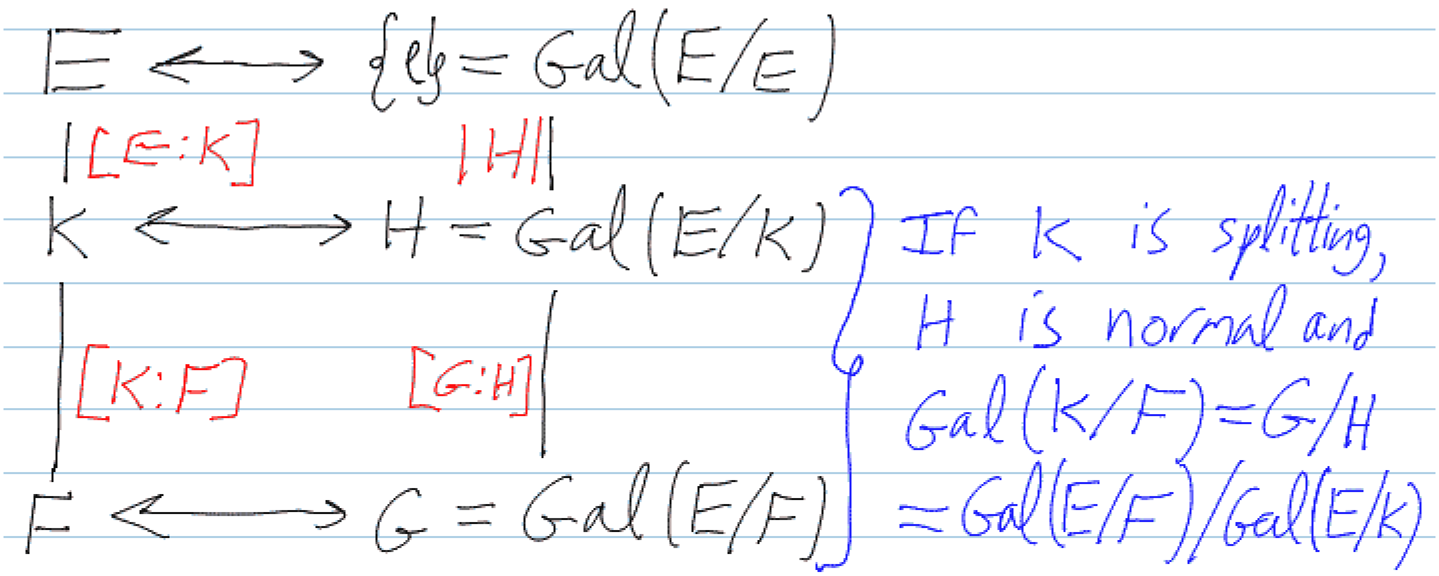
and reversely, by mapping every subgroup H of $\operatorname{Gal}(E/F)$ to its fixed field E_H:

$$\Psi: \quad H\mapsto E_H := \{x\in E : \forall h\in H,\ hx=x\}.$$

This correspondence has the following further properties:

1. It is inclusion-reversing: if $H_1\subset H_2$ then $E_{H_1}\supset E_{H_2}$ and if $K_1\subset K_2$ then $\operatorname{Gal}(E/K_1)>\operatorname{Gal}(E/K_2)$.
2. It is degree/index respecting: $[E:K]=|\operatorname{Gal}(E/K)|$ and $[K:F]=[\operatorname{Gal}(E/F):\operatorname{Gal}(E/K)]$.

3. Splitting fields correspond to normal subgroups: If K in $E/K/F$ is the splitting field of a polynomial in $F[x]$ then $\text{Gal}(E/K)$ is normal in $\text{Gal}(E/F)$ and $\text{Gal}(K/F) \cong \text{Gal}(E/F)/\text{Gal}(E/K)$.



The Fundamental Theorem of Galois Theory, all in one.

Lemmas

The four lemmas below belong to earlier chapters but we skipped them in class (the last one was also skipped by Gallian).

Zeros of Irreducible Polynomials

Lemma 1. An irreducible polynomial over a field of characteristic 0 has no multiple roots.

Proof. See the proof of Theorem 20.6 on page 362 of Gallian's book. □

Uniqueness of Splitting Fields

Lemma 2. Let $\phi : F_1 \to F_2$ be an isomorphism of fields, let $f_1 \in F_1[x]$ be a polynomial and let $f_2 = \phi(f_1)$, and let E_1 and E_2 be splitting fields for f_1 and f_2 over F_1 and F_2, respectively. Then there is an isomorphism $\bar{\phi} : E_1 \to E_2$ (generally not unique) that extends ϕ.

Proof. See the proof of Theorem 20.4 on page 360 of Gallian's book. □

The Primitive Element Theorem

The celebrated "Primitive Element Theorem" is just a lemma for us:

Lemma 3. Let a and b be algebraic elements of some extension E of F. Then there exists a single element c of E so that $F(a, b) = F(c)$. (And so by induction, every finite extension of E is "simple", meaning, is generated by a single element, called "a primitive element" for that extension).

Proof. See the proof of Theorem 21.6 on page 375 of Gallian's book. □

Splitting Fields are Good at Splitting

Lemma 4. (Compare with Hungerford's Theorem 10.15 on page 355). If E is a splitting field of some polynomial f over F and some irreducible polynomial $p \in F[x]$ has a root v in E, then p splits in E.

Proof. Let L be a splitting field of p over E. We need to show that if w is a root of p in L, then $w \in E$ (so all the roots of p are in E and hence p splits in E). Consider the two extensions

$$E = E(v)/F(v) \text{ and } E(w)/F(w).$$

The "smaller fields" $F(v)$ and $F(w)$ in these two extensions are isomorphic as they both arise by adding a root of the same irreducible polynomial (p) to the base field F. The "larger fields" $E = E(v)$ and $E(w)$ in these two extensions are both the splitting fields of the same polynomial (f) over the respective "small fields", as E/F is a splitting extension for f and we can use the sub-lemma below. Thus by the uniqueness of splitting extensions (lemma 2), the isomorphism between $F(v)$ and $F(w)$ extends to an isomorphism between $E = E(v)$ and $E(w)$, and in particular these two fields are isomorphic and so $[E : F] = [E(v) : F] = [E(w) : F]$. Since all the degrees involved are finite it follows from the last equality and from $[E(w) : F] = [E(w) : E][E : F]$ that $[E(w) : E] = 1$ and therefore $E(w) = E$. Therefore $w \in E$. □

Sub-lemma. If E/F is a splitting extension of some polynomial $f \in F[x]$ and z is an element of some larger extension L of E, then $E(z)/F(z)$ is also a splitting extension of f.

Proof. Let $u_1, \ldots, u_n$ be all the roots of f in E. Then they remain roots of f in $E(z)$, and since f completely splits already in E, these are *all* the roots of f in $E(z)$. So

$$E(z) = F(u_1, \ldots, u_n)(z) = F(z)(u_1, \ldots, u_n),$$

and $E(z)$ is obtained by adding all the roots of f to $F(z)$. □

Proof of The Fundamental Theorem

The Bijection

Proof of $\Psi \circ \Phi = I$. More precisely, we need to show that if K is an intermediate field between E and F, then $E_{\mathrm{Gal}(E/K)} = K$. The inclusion $E_{\mathrm{Gal}(E/K)} \supset K$ is easy, so we turn to prove the other inclusion. Let $v \in E - K$ be an element of E which is not in K. We need to show that there is some automorphism $\phi \in \mathrm{Gal}(E/K)$ for which $\phi(v) \neq v$; if such a ϕ exists it follows that $v \notin E_{\mathrm{Gal}(E/K)}$ and this implies the other inclusion. So let p be the minimal polynomial of v over K. It is not of degree 1; if it was, we'd have that $v \in K$ contradicting the choice of v . By lemma 4 and using the fact that E is a splitting extension, we know that p splits in E, so E contains all the roots of p. Over a field of characteristic 0 irreducible polynomials cannot have multiple roots (lemma 1) and hence p must have at least one other root; call it w. Since v and w have the same minimal polynomial over K, we know that $K(v)$ and $K(w)$ are isomorphic; furthermore, there is an isomorphism $\phi_0 : K(v) \to K(w)$ so that $\phi_0|_K = I$ yet $\phi_0(v) = w$. But E is a splitting field of some polynomial f over F and hence also over $K(v)$ and over $K(w)$. By the uniqueness of splitting fields (lemma 2), the isomorphism ϕ_0 can be extended to an isomorphism $\phi : E \to E$; i.e., to an automorphism of E. but then $\phi|_K = \phi_0|_K = I$ so $\phi \in \mathrm{Gal}(E/K)$, yet $\phi(v) = w \neq v$, as required. □

Proof of $\Phi \circ \Psi = I$. More precisely we need to show that if $H < \operatorname{Gal}(E/F)$ is a subgroup of the Galois group of E over F, then $H = \operatorname{Gal}(E/E_H)$. The inclusion $H < \operatorname{Gal}(E/E_H)$ is easy. Note that H is finite since we've proven previously that Galois groups of finite extensions are finite and hence $\operatorname{Gal}(E/F)$ is finite. We will prove the following sequence of inequalities:

$$|H| \leq |\operatorname{Gal}(E/E_H)| \leq [E:E_H] \leq |H|$$

This sequence and the finiteness of $|H|$ imply that these quantities are all equal and since $H < \operatorname{Gal}(E/E_H)$ it follows that $H = \operatorname{Gal}(E/E_H)$ as required.

The first inequality above follows immediately from the inclusion $H < \operatorname{Gal}(E/E_H)$.

By the Primitive Element Theorem (Lemma 3) we know that there is some element $u \in E$ so that $E = E_H(u)$. Let p be the minimal polynomial of u over E_H. Distinct elements of $\operatorname{Gal}(E/E_H)$ map u to distinct roots of p, but p has exactly $\deg p$ roots. Hence $|\operatorname{Gal}(E/E_H)| \leq \deg p = [E:E_H]$, proving the second inequality above.

Let $\sigma_1, \dots, \sigma_n$ be an enumeration of all the elements of H, let $u_i := \sigma_i u$ (with u as above), and let f be the polynomial

$$f = \prod_{i=1}^{n}(x - u_i).$$

Clearly, $f \in E[x]$. Furthermore, if $\tau \in H$, then left multiplication by τ permutes the σ_i's (this is always true in groups), and hence the sequence $(\tau u_i = \tau\sigma u_i)_{i=1}^n$ is a permutation of the sequence $(u_i)_{i=1}^n$, hence

$$\tau f = \prod_{i=1}^{n}(x - \tau u_i) = \prod_{i=1}^{n}(x - u_i) = f,$$

and hence $f \in E_H[x]$. Clearly $f(u) = 0$, so $p|f$, so $[E:E_H] = \deg p \leq \deg f = n = |H|$, proving the third inequality above. $\square$

The Properties

Property 1. If $H_1 \subset H_2$ then $E_{H_1} \supset E_{H_2}$ and if $K_1 \subset K_2$ then $\operatorname{Gal}(E/K_1) > \operatorname{Gal}(E/K_1)$.

Proof of Property 1. Easy. $\square$

Property 2. $[E:K] = |\operatorname{Gal}(E/K)|$ and $[K:F] = [\operatorname{Gal}(E/F) : \operatorname{Gal}(E/K)]$.

Proof of Property 2. If $K = E_H$, then $|\operatorname{Gal}(E/K)| = |\operatorname{Gal}(E/E_H)| = [E:E_H] = [E:K]$ as was shown within the proof of $\Phi \circ \Psi = I$. But every K is E_H for some H, so $|\operatorname{Gal}(E/K)| = [E:K]$ for every K between E and F. The second equality follows from the first and from the multiplicativity of the degree/order/index in towers of extensions and in towers of groups:

$$[K:F] = \frac{[E:F]}{[E:K]} = \frac{|\operatorname{Gal}(E/F)|}{|\operatorname{Gal}(E/K)|} = [\operatorname{Gal}(E/F) : \operatorname{Gal}(E/K)]. \quad \square$$

Property 3. If K in $E/K/F$ is the splitting field of a polynomial in $F[x]$ then $\operatorname{Gal}(E/K)$ is normal in $\operatorname{Gal}(E/F)$ and $\operatorname{Gal}(K/F) \cong \operatorname{Gal}(E/F)/\operatorname{Gal}(E/K)$.

Proof of Property 3. We will define a surjective (onto) group homomorphism $\rho : \mathrm{Gal}(E/F) \to \mathrm{Gal}(K/F)$ whose kernel is $\mathrm{Gal}(E/K)$. This shows that $\mathrm{Gal}(E/K)$ is normal in $\mathrm{Gal}(E/F)$ (kernels of homomorphisms are always normal) and then by the first isomorphism theorem for groups, we'll have that $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F)/\,\mathrm{Gal}(E/K)$.

Let σ be in $\mathrm{Gal}(E/F)$ and let u be an element of K. Let p be the minimal polynomial of u in $F[x]$. Since K is a splitting field, lemma 4 implies that p splits in $K[x]$, and hence all the other roots of p are also in K. As $\sigma(u)$ is a root of p, it follows that $\sigma(u) \in K$ and hence $\sigma(K) \subset K$. But since σ is an isomorphism, $[\sigma(K) : F] = [K : F]$ and hence $\sigma(K) = K$. Hence the restriction $\sigma|_K$ of σ to K is an automorphism of K, so we can define $\rho(\sigma) = \sigma|_K$.

Clearly, ρ is a group homomorphism. The kernel of ρ is those automorphisms of E whose restriction to K is the identity. That is, it is $\mathrm{Gal}(E/K)$. Finally, as E/F is a splitting extension, so is E/K. So every automorphism of K extends to an automorphism of E by the uniqueness statement for splitting extensions (lemma 2). But this means that ρ is onto. $\square$