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 $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(E/F)/\mathrm{Gal}(E/K)$.