Section V.2. The Fundamental Theorem of Galois Theory (Supplement)

Some Field Extension Observations

Recall. If F is an extension field of field K then F is a vector space over K (see page 231).

Theorem V.1.11. If F is a finite dimensional (vector space) extension field of K, then F is finitely generated and algebraic over K.

Note. We have:

- $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a finitely generated extension of $\mathbb{Q}$ (generated by $X = \{\sqrt{2}, \sqrt{3}\}$ over $\mathbb{Q}$) and finite dimensional, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.
- $\mathbb{Q}(\pi) \cong \mathbb{Q}(x)$ (by Theorem V.1.5) is a finitely generated extension of $\mathbb{Q}$ (with $X = \{\pi\}$; in fact, it's a simple extension). It is not an algebraic extension (since π is not algebraic) and is not a finite dimensional extension of $\mathbb{Q}$ (since the set $X = \{1, \pi, \pi^2, \pi^3, \ldots\}$ is linearly independent).
- $\mathbb{Q}(\sqrt[3]{2})$ is an algebraic extension, a simple extension, and $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ (by Theorem V.1.6).
- The algebraic real numbers, $\mathbb{A}_{\mathbb{R}}$, are an algebraic extension of $\mathbb{Q}$. But $\mathbb{A}_{\mathbb{R}}$ is not a finitely generated extension (consider the set $\{\sqrt[p]{2} \mid p \in \mathbb{N} \text{ is prime}\}$) nor

a finite dimensional extension of $\mathbb{Q}$ (the set $X = \{\sqrt{p} \mid p \in \mathbb{N} \text{ is prime}\}$ is linearly independent). The same holds for the algebraic complex numbers, $\mathbb{A}_{\mathbb{C}}$.

- $\mathbb{C} = \mathbb{R}(i)$ is a finite dimensional, finitely generated (simple, in fact), algebraic extension of $\mathbb{R}$.
- $\mathbb{R}$ is an infinite dimensional, infinitely generated, non algebraic extension of $\mathbb{Q}$.

Some Galois Extension Observations

Recall. F is a Galois extension field of field K if the fixed field of $\mathrm{Aut}_K(F)$ is K itself; that is, $K = (\mathrm{Aut}_k(F))'$ (Definition V.2.4).

Exercise V.2.9. (a) If K is an infinite field, then $K(x)$ is Galois over K.

Proof. ASSUME that $K(x)$ is not Galois over K. Then by the definition of Galois, the fixed field of $\mathrm{Aut}_K K(x)$ does not equal K, $(\mathrm{Aut}_K K(x))' = E \neq K$. Then we have $K(x) \supseteq E \supseteq K$ and $E \neq K$, so by Exercise V.2.6(b), we have that $[K(x) : E]$ is finite. Now $\mathrm{Aut}_E K(x) = \mathrm{Aut}_K K(x)$ and by Exercise V.2.6(d), since K is an infinite field, then $\mathrm{Aut}_K K(x) = \{(ax+b)/(cx+d) \mid a,b,c,d \in K, ad-bc \neq 0\}$ is infinite. Therefore $\mathrm{Aut}_E K(x) = \mathrm{Aut}_K K(x)$ is infinite. But then by Lemma V.2.8 (the "in particular" part) we have $|\mathrm{Aut}_E K(x)| \leq [K(x) : E]$, a CONTRADICTION. So the assumption that $K(x)$ is not Galois over K is false and hence $K(x)$ is Galois over K. ∎

(b) If K is finite, then $K(x)$ is not Galois over K. HINT: Prove by contradiction. Use Exercise V.2.6(d) to show that $\text{Aut}_K K(x)$ is finite. Use Theorem V.1.5 and Theorem V.1.11 to show that $[K(x) : K]$ is infinite. Use Lemma V.2.9 to get a contradiction.

Proof. ASSUME $K(x)$ is Galois over K. Then the fixed field of $\text{Aut}_K K(x)$ is $(\text{Aut}_K K(x))' = K$. By Exercise V.2.6(d), every element of $\text{Aut}_K K(x)$ is induced by a mapping $x \mapsto (ax+b)/(cx+d)$ where $a, b, c, d \in K$ and $ad - bc \neq 0$. Since K is finite, then there are only a finite number of such mappings and hence

$$\text{Aut}_K K(x) \text{ is finite.} \qquad (*)$$

Now x is transcendental over K by Theorem V.1.5, so by the contrapositive of Theorem V.1.11,

$$[K(x) : K] \text{ is infinite.} \qquad (**)$$

Let $J = \text{Aut}_K K(x)$ and $H = \{1_{K(x)}\} < \text{Aut}_K K(x) = J$. Then the fixed field of H is $H' = K(x)$ and as assumed above the fixed field of $J = \text{Aut}_K K(x)$ is $J' = K$. By Lemma V.2.9, $[H' : J'] \leq [J : H]$ or $[K(x) : K] \leq [\text{Aut}_K K(x) : \{1_{K(x)}\}]$. But $[\text{Aut}_K K(x) : \{1_{K(x)}\}] = |\text{Aut}_K K(x)|$ is finite by $(*)$ and $[K(x) : K]$ is infinite by $(**)$, a CONTRADICTION. So the assumption that $K(x)$ is Galois over K is false and so $K(x)$ is not Galois over K. ∎

Note. We have:

- $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a Galois extension of $\mathbb{Q}$ and $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}, \sqrt{3})) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.
- $\mathbb{Q}(\pi) \cong \mathbb{Q}(x)$ is Galois over $\mathbb{Q}$ by Exercise V.2.9 (in fact, this holds for any infinite base field K). Notice that $\mathbb{Q}(\pi)$ is not an algebraic extension of $\mathbb{Q}$.

- $\mathbb{Q}(\sqrt[3]{2})$ is not a Galois extension of $\mathbb{Q}$ (see the first example on page 244 or the first example on page 4 of the class notes). The fixed field of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Q}(\sqrt[3]{2})$.

- $\mathbb{C} = \mathbb{R}(i)$ is a Galois extension of $\mathbb{R}$ and $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) \cong \mathbb{Z}_2$.

- $\mathbb{R}$ is not a Galois extension of $\mathbb{Q}$ since the fixed field of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{R})$ is $\mathbb{R}$ by Exercise V.2.2.

- The algebraic complex numbers $\mathbb{Q}_{\mathbb{C}}$ are Galois over $\mathbb{Q}$. (If $u \in \mathbb{A}_{\mathbb{C}}$ and $u \not\in \mathbb{Q}$ then $p(u) = 0$ for some $p \in \mathbb{Q}[x]$ where p is irreducible and $\deg(p) \geq 2$. Since $\deg(p) \geq 2$, then there is $v \in \mathbb{A}_{\mathbb{C}}$ where $p(v) = 0$ and $v \neq u$. By Corollary V.1.9, there is $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{A}_{\mathbb{C}})$ where $\sigma(u) = v$ where $p(v) = 0$ and $v \neq u$.)

- The algebraic real numbers, $\mathbb{A}_{\mathbb{R}}$, are no Galois over $\mathbb{Q}$. For $\sqrt[2]{3} \in \mathbb{A}_{\mathbb{R}}$ the same argument given for $\mathbb{Q}(\sqrt[3]{2})$ shows that $\sqrt[3]{2}$ must be fixed by all $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{A}_{\mathbb{R}})$ and so the fixed field of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{A}_{\mathbb{R}})$ is not $\mathbb{Q}$.

Revised: 4/9/2016