

V. FIELDS AND GALOIS THEORY

V.2. The Fundamental Theorem.

4. What is the Galois group of $F = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ over \mathbb{Q} ?

Since F is generated over \mathbb{Q} by $\{1, \sqrt{2}, \sqrt{3}, \sqrt{5}\}$, we need to determine all possible images $\sigma(\sqrt{2}), \sigma(\sqrt{3}), \sigma(\sqrt{5})^1$ for $\sigma \in \text{Aut}_{\mathbb{Q}}F$. Now

$$\sqrt{2} \text{ has irreducible polynomial } f(x) = x^2 - 2 \in \mathbb{Q}[x]$$

$$\sqrt{3} \text{ has irreducible polynomial } g(x) = x^2 - 3 \in \mathbb{Q}[x]$$

$$\sqrt{5} \text{ has irreducible polynomial } h(x) = x^2 - 5 \in \mathbb{Q}[x]$$

Since σ must take roots of f to roots of f (etc.), we must have

$$\sigma(\sqrt{2}) = \pm\sqrt{2} \qquad \sigma(\sqrt{3}) = \pm\sqrt{3} \qquad \sigma(\sqrt{5}) = \pm\sqrt{5}$$

Since we have three independent binary choices, $\text{Aut}_{\mathbb{Q}}F = \mathbb{Z}^2 \oplus \mathbb{Z}^2 \oplus \mathbb{Z}^2$.

To verify this formally, note that $|\text{Aut}_{\mathbb{Q}}F| = 8$ and every element u of $\text{Aut}_{\mathbb{Q}}F$ has order $|u| \leq 2$. ■

6. Let $\frac{f}{g} \in K(x)$ with $\frac{f}{g} \notin K$ and f, g relatively prime in $K[x]$ and consider the extension of K by $K(x)$.

- a) x is algebraic over $K(\frac{f}{g})$ and $[K(x) : K(\frac{f}{g})] = \max(\deg f, \deg g)$.

Since f/g is transcendental over K , we write $f/g = z$ and consider z as an indeterminate. Let the polynomial $\varphi \in K(z)[y]$ be defined by $\varphi(y) = zg(y) - f(y)$ so that x is clearly a root of φ . First we show that it is primitive and irreducible over $K[z][y] = K[z, y]$, and then use III.6.13.

φ is irreducible in $K[z][y]$. Suppose φ were reducible: but then

$\varphi(y) = (zg_1(y) - f_1(y))h$ (where $f_1h = f$ and $g_1h = g$), $\not\sim f, g$ are relatively prime.

φ is primitive. Suppose not: then for

$$\varphi(y) = (zb_0 - a_0) + (zb_1 - a_1)y + \dots + (zb_n - a_n)y^n$$

there would be $r \in K$ such that $zb_i - a_i = b_i(z - r)$, which implies $a_i = rb_i, \forall i$. But this would mean $\frac{f}{g} = r \in K$, $\not\sim$ hypothesis.

Now that φ is a primitive irreducible polynomial, we know φ is irreducible over $K(z)[y]$ by III.6.13. Hence, φ is the irreducible polynomial of x and x is thus algebraic over $K(\frac{f}{g})$. By examination of φ , it is also clear that

$$[K(x) : K(\frac{f}{g})] = \deg \varphi = \max(\deg f, \deg g). \quad \blacksquare$$

¹Since σ fixes K , we know that we must have $\sigma(1) = 1$.

b) If $E \neq K$ is an intermediate field of the extension $K(x) : K$, then

$$[K(x) : E] < \infty.$$

$E \neq K$, so pick $u \in E \setminus K$. Then $u \in E$ implies that u is of the form $\frac{f(x)}{g(x)}$, for some $f, g \in K[x] \setminus K$. x is algebraic over $K(u)$ by part (a), because $E \neq K \implies \frac{f}{g} \notin K$ and we can choose f, g coprime. Let h be the irreducible polynomial of x over $K(u)$. Then we have a tower of fields

$$K(x) \supseteq E \supseteq K(h) \supseteq K$$

and a corresponding product of dimensions

$$[K(x) : K(u)] = [K(x) : E] [E : K(u)].$$

Since $[K(x) : K(u)] = \deg h < \infty$, this clearly implies $[K(x) : E] < \infty$. ■

c) $x \mapsto \frac{f}{g}$ induces a homomorphism such that $\sigma : \frac{\varphi(x)}{\psi(x)} \mapsto \varphi(f/g)/\psi(f/g)$.
 $\sigma \in \text{Aut}_K F \iff \max(\deg f, \deg g) = 1$.

To see that σ induces the given homomorphism, use the proof of 2.2. Note that σ is a field homomorphism, so it is certainly injective by III.2.21(iv). Now,

$$\begin{aligned} \max(\deg f, \deg g) = 1 &\iff [K(x) : K\left(\frac{f}{g}\right)] = 1 && \text{by (a)} \\ &\iff K(x) = K\left(\frac{f}{g}\right) = \sigma(K(x)) \\ &\iff \sigma \text{ is surjective.} \end{aligned}$$

■

d) $\text{Aut}_K K(x) = \{x \mapsto \frac{ax+b}{cx+d} : a, b, c, d \in K \text{ and } ad - bc \neq 0\} = GL_2(K)$.

First note that the map $\frac{\varphi(x)}{\psi(x)} \mapsto \frac{\varphi(f/g)}{\psi(f/g)}$ discussed previously is just evaluation at $\frac{f}{g}$ and thus fixes K . Then

$$\sigma \in \text{Aut}_K K(x) \iff \sigma \in GL_2(K)$$

follows immediately from (c) and the fact that

$$\sigma \text{ is invertible} \iff ad - bc \neq 0.$$

For $a \in K \setminus \{0\}, b \in K$, the maps

$$\begin{array}{ccc} \sigma_a : K(x) \rightarrow K(x) & & \tau_b : K(x) \rightarrow K(x) \\ \text{by } \sigma_a : \frac{f(x)}{g(x)} \mapsto \frac{f(ax)}{g(ax)} & \text{and} & \text{by } \tau_b : \frac{f(x)}{g(x)} \mapsto \frac{f(x+b)}{g(x+b)} \end{array}$$

are clearly K -automorphisms of $K(x)$. ■

9. a) If K is infinite, then $K(x)$ is Galois over K .

If $K(x)$ is not Galois over K , then $K \neq \mathcal{F}(\text{Aut}_K K(x))$, so we must have $K \subsetneq E = \mathcal{F}(\text{Aut}_K K(x))$. Then $[K(x) : E] < \infty$ by 6(b), which implies that

$$\begin{aligned} [\text{Aut}_E K(x) : \text{Aut}_{K(x)} K(x)] &= [\text{Aut}_E K(x) : 1] \\ &= |\text{Aut}_E K(x)| \\ &\leq [K(x) : E] && \text{by Lemma 2.8} \\ &< \infty \end{aligned}$$

By hypothesis, $|K| = \infty$, so $|\text{Aut}_K K(x)| = \left| \left\{ \frac{ax+b}{cx+d} \right\} \right| = \infty$ by 6(d). But then Lemma 2.6(iv) gives

$$\text{Aut}_K K(x) = \text{Aut}_E K(x)$$

which then implies

$$|\text{Aut}_E K(x)| = \infty$$

\succ above. ■

b) If K is finite, then $K(x)$ is not Galois over K .

First note that, as above, $\text{Aut}_K K(x) = \frac{ax+b}{cx+d}$ by 6(d), so

$$|K| = n < \infty \implies |\text{Aut}_K K(x)| \leq n^4 < \infty$$

By hypothesis, $[\text{Aut}_K K(x) : 1_K] < \infty$, so

$$[\mathcal{F}(1_K) : \mathcal{F}(\text{Aut}_K K(x))] \leq [\text{Aut}_K K(x) : 1_K]$$

by Lemma 2.9. If $K(x)$ were Galois, this would imply

$$[K(x) : K] \leq |\text{Aut}_K K(x)| \leq n^4 < \infty$$

\succ x is transcendental. ■

11. In the extension of \mathbb{Q} by $\mathbb{Q}(x)$, show that the intermediate field $\mathbb{Q}(x^2)$ is closed, but $\mathbb{Q}(x^3)$ is not.

a) $\mathbb{Q}(x^2)$ is closed $\iff \forall u \in \mathbb{Q}(x) \setminus \mathbb{Q}(x^2), \exists \sigma \in \text{Aut}_{\mathbb{Q}(x^2)}\mathbb{Q}(x)$ such that $\sigma(u) \neq u$.

Note that $\mathbb{Q}(x)$ is algebraic over $\mathbb{Q}(x^2)$ with basis $\{1, x\}$, because x is a root of $f(y) = y^2 - x^2 \in \mathbb{Q}(x^2)[y]$. Then pick $u \in \mathbb{Q}(x) \setminus \mathbb{Q}(x^2)$, so $u = a + bx$ where $b \neq 0$. Let σ be defined by $\sigma(1) = 1, \sigma(x) = -x$. Now $\sigma(u) = a - bx \neq u$, but for any $v \in \mathbb{Q}(x^2)$, define $v = \sum_{i=0}^n a_i x^{2i}$ so that

$$\begin{aligned} \sigma(v) &= \sum_{i=0}^n \sigma(a_i) \sigma(x)^{2i} \\ &= \sum_{i=0}^n a_i (-x)^{2i} \\ &= \sum_{i=0}^n a_i x^{2i} \\ &= v \end{aligned}$$

Thus, σ fixes $\mathbb{Q}(x^2)$ but not u . ■

b) To see that $\mathbb{Q}(x^3)$ is not closed, we will exhibit $u \in \mathbb{Q}(x) \setminus \mathbb{Q}(x^3)$ which is fixed by any $\sigma \in \text{Aut}_{\mathbb{Q}(x^3)}\mathbb{Q}(x)$. Let $u = x + x^3$ so that $\sigma(u) = \sigma(x) + x^3$ because σ fixes $x^3 \in \mathbb{Q}(x^3)$. We note that $\mathbb{Q}(x)$ is algebraic over $\mathbb{Q}(x^3)$ with basis $\{1, x, x^2\}$, because x is a root of $f(y) = y^3 - x^3 \in \mathbb{Q}(x^3)[y]$. So σ is completely determined by its action on $\{1, x\}$.

We know that $\sigma(1) = 1$ as above (because σ must fix $\mathbb{Q}(x^3)$), but what is $\sigma(x)$? $\sigma(x)$ must be a root of $f(y)$, but $f(y)$ has only one root: x . Thus, $\sigma(x) = x \implies \sigma(u) = x + x^3 = u$, for any σ which fixes $\mathbb{Q}(x^3)$.

Thus, $u \in \mathcal{F}(\text{Aut}_{\mathbb{Q}(x^3)}\mathbb{Q}(x)) \setminus \mathbb{Q}(x^3) \implies \mathcal{F}(\text{Aut}_{\mathbb{Q}(x^3)}\mathbb{Q}(x)) \neq \mathbb{Q}(x^3)$, i.e., $\mathbb{Q}(x^3)$ is not closed. ■

14. Let $F : K$ be a finite-dimensional Galois extension with intermediate fields L, M .

a) $\text{Aut}_{LM}F = \text{Aut}_L F \cap \text{Aut}_M F$

LM is the smallest field containing L and M means that

$$L \subseteq LM, M \subseteq LM \text{ and } L, M \subseteq E \implies LM \subseteq E$$

We proceed to show the equality by a double-inclusion argument.

\square $L \subseteq LM \implies \text{Aut}_{LM}F \subseteq \text{Aut}_L F$, and $M \subseteq LM \implies \text{Aut}_{LM}F \subseteq \text{Aut}_M F$, so clearly $\text{Aut}_{LM}F \subseteq \text{Aut}_L F \cap \text{Aut}_M F$.

\square Making extensive use of the fact that $F : K$ is f.d.g.,

$$\begin{aligned} \text{Aut}_L F \cap \text{Aut}_M F &\subseteq \text{Aut}_L F, \text{Aut}_M F \\ &\implies \mathcal{F}(\text{Aut}_L F), \mathcal{F}(\text{Aut}_M F) \subseteq \mathcal{F}(\text{Aut}_L F \cap \text{Aut}_M F) \\ &\implies L, M \subseteq \mathcal{F}(\text{Aut}_L F \cap \text{Aut}_M F) && \text{Lemma 2.10} \\ &\implies LM \subseteq \mathcal{F}(\text{Aut}_L F \cap \text{Aut}_M F) && \text{by first line} \\ &\implies \text{Aut}_{\mathcal{F}(\text{Aut}_L F \cap \text{Aut}_M F)} F \subseteq \text{Aut}_{LM} F && \text{by Fun. Thm.} \\ &\implies \text{Aut}_L F \cap \text{Aut}_M F \subseteq \text{Aut}_{LM} F && \text{Lemma 2.6(iii)} \end{aligned}$$

b) $\text{Aut}_{L \cap M} F = \text{Aut}_L F \vee \text{Aut}_M F$

\square $L \cap M \subseteq L, M \implies \text{Aut}_L F, \text{Aut}_M F \subseteq \text{Aut}_{L \cap M} F \implies \text{Aut}_L F \vee \text{Aut}_M F \subseteq \text{Aut}_{L \cap M} F$, because the join is the smallest group containing both $\text{Aut}_L F$ and $\text{Aut}_M F$.

\square $\mathcal{F}(\text{Aut}_{L \cap M} F) = L \cap M$ by f.d.g., so

$$\begin{aligned} \text{Aut}_L F, \text{Aut}_M F &\subseteq \text{Aut}_L F \vee \text{Aut}_M F && \text{def of } \vee \\ &\implies \mathcal{F}(\text{Aut}_L F \vee \text{Aut}_M F) \subseteq \mathcal{F}(\text{Aut}_L F, \text{Aut}_M F) && \text{by Fun. Thm.} \\ &\implies \mathcal{F}(\text{Aut}_L F \vee \text{Aut}_M F) \subseteq L, M && \text{by f.d.g.} \\ &\implies \mathcal{F}(\text{Aut}_L F \vee \text{Aut}_M F) \subseteq L \cap M \end{aligned}$$

c) What conclusion can be drawn if $\text{Aut}_L F \cap \text{Aut}_M F = 1$?

In this case,

$$\begin{aligned} \text{Aut}_L F \cap \text{Aut}_M F &= \text{Aut}_{LM} F = 1 && \text{by above} \\ &\implies \mathcal{F}(\text{Aut}_{LM} F) = \mathcal{F} && \text{by Fun. Thm.} \\ &\implies LM = F && \text{by f.d.g.} \end{aligned}$$

15. a) $F : K$ is a finite-dimensional Galois extension with intermediate field $E \implies \exists! L$ where L is the smallest field such that $E \subseteq L \subseteq F$ and L is Galois over K .

Let $\{L_i\}$ be the set of Galois extensions of K which contain E . Since $[F : K] < \infty$, there are a finite number of them. Now define $L = \bigcap_{i=1}^n L_i$ so that L is the smallest extension of K containing E . To see that $L : K$ is Galois, consider the corresponding subgroups $\text{Aut}_{L_i} F$. We have $\text{Aut}_{L_i} F \triangleleft \text{Aut}_K F$ for each L_i , by the Fun. Thm., and

$$\text{Aut}_L F = \text{Aut}_{\bigcap_{i=1}^n L_i} F = \bigcap_{i=1}^n \text{Aut}_{L_i} F$$

follows by #14(b). Now we have

$$\bigcap_{i=1}^n \text{Aut}_{L_i} F \triangleleft \text{Aut}_K F$$

by exercise I.5.3(a) (with a brief induction). Then $\text{Aut}_L F \triangleleft G \implies L : K$ is Galois by the Fun. Thm. again.

b) Furthermore, $\text{Aut}_L F = \bigcap_{\sigma} \sigma (\text{Aut}_E F) \sigma^{-1}$ where σ runs over all of $\text{Aut}_K F$.

□ To see $\text{Aut}_L F \subset \bigcap_{\sigma} \sigma (\text{Aut}_E F) \sigma^{-1}$,

$$\begin{aligned} \text{Aut}_L F &= \sigma (\text{Aut}_L F) \sigma^{-1} \quad \forall \sigma & \text{Aut}_L F &\triangleleft \text{Aut}_K F \\ &\subset \sigma (\text{Aut}_E F) \sigma^{-1} \quad \forall \sigma & \text{Aut}_L F &\subset \text{Aut}_E F \\ &\subset \bigcap_{\sigma \in \text{Aut}_K F} \sigma (\text{Aut}_E F) \sigma^{-1} \end{aligned}$$

□ Now to see $\bigcap_{\sigma} \sigma (\text{Aut}_E F) \sigma^{-1} \subset \text{Aut}_L F$.

We know that $\text{Aut}_L F = \bigvee \text{Aut}_{L_i} F$, so it suffices to show that $\bigcap_{\sigma} \sigma (\text{Aut}_E F) \sigma^{-1} \subset \text{Aut}_{L_i} F$ for some i , i.e., that $\bigcap_{\sigma} \sigma (\text{Aut}_E F) \sigma^{-1}$ is normal in $\text{Aut}_K F$ and contained in $\text{Aut}_E F$.

To see $\bigcap_{\sigma} \sigma (\text{Aut}_E F) \sigma^{-1} \triangleleft \text{Aut}_K F$, pick $\tau \in \text{Aut}_K F$. Then

$$\begin{aligned} \tau \left(\bigcap_{\sigma} \sigma (\text{Aut}_E F) \sigma^{-1} \right) \tau^{-1} &= \bigcap_{\sigma} \tau (\sigma (\text{Aut}_E F) \sigma^{-1}) \tau^{-1} \\ &= \bigcap_{\sigma} \tau \sigma (\text{Aut}_E F) (\tau \sigma)^{-1} \\ &= \bigcap_{\rho} \rho (\text{Aut}_E F) \rho^{-1} \\ &= \bigcap_{\sigma} \sigma (\text{Aut}_E F) \sigma^{-1}. \end{aligned}$$

To see why the last steps hold, consider that the intersection runs over all permutations $\sigma \in \text{Aut}_K F$, but it doesn't matter in which order. Putting $\sigma\tau = \rho$ amounts to shuffling the indices and reordering them in their original state. Now $\bigcap_{\sigma} \sigma (\text{Aut}_E F) \sigma^{-1}$ is invariant under conjugation and hence normal, which means that $\bigcap_{\sigma} \sigma (\text{Aut}_E F) \sigma^{-1} = \text{Aut}_{L_j} F$ for some j . Thus,

$$\begin{aligned} \bigcap_{\sigma} \sigma (\text{Aut}_E F) \sigma^{-1} &\subseteq \bigvee \text{Aut}_{L_i} F \\ &= \text{Aut}_{\cap L_i} F \\ &= \text{Aut}_L F. \end{aligned}$$