# V. Fields and Galois Theory

## V.1. **Field Extensions.**

7. If $v$ is algebraic over $K(u)$ for some $u \in F$ and $v$ is transcendental over $K$, then $u$ is algebraic over $K(v)$.

   If $v$ is algebraic over $K(u)$, then $\exists f(x) \in K(u)[x]$ such that $f(v) = 0$. Let
   $$f(x) = \sum_{i=0}^{n} \tfrac{g_i(u)}{h_i(u)} x^i$$
   where $g_i(x) = \sum_{j=0}^{m} a_{ij} x^j$, for $a_{ij} \in K, \forall i, j$. Then
   $$f(v) = 0 \implies \sum g_i(u) v^i = 0 \implies g_i(u) = 0, \ \forall i$$
   because the $v^i$ are linearly independent. Then
   $$\begin{aligned} 0 &= \sum_{i=0}^{n} g_i(u) v^i \\ &= \sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} u^j v^i \\ &= \sum_{j=0}^{m} \sum_{i=0}^{n} a_{ij} u^j v^i \\ &= \sum_{j=0}^{m} \phi_j(v) u^j \end{aligned}$$
   where $\phi_j(v) = \sum_{i=0}^{n} a_{ij} v^i$, where $a_{ij} \in k$. We know that $\phi_j(v) \neq 0$ because $v$ is transcendental over $K$. This tells us that
   $$\psi(x) = \sum_{j=0}^{m} \phi_j(v) x^j \in K(v)[x]$$
   is a nonzero polynomial. Since $\psi(u) = 0$, $u$ is algebraic over $K(v)$. ■

8. If $u \in F$ is algebraic of odd degree over $K$, then so is $u^2$ and $K(u) = K(u^2)$.

   Was this one even assigned?

9. If $f(x) = x^n - a \in K[x]$ is irreducible and $u \in F$ is a root of $f$ and $m|n$, then prove that the degree of $u^m$ over $K$ is $\frac{n}{m}$. What is the irreducible polynomial for $u^m$ over $K$?

   Since $n|m$,
   $$h(x) = x^{n/m} - a$$
   is a polynomial in $K[x]$. Then
   $$h(u^m) = (u^m)^{n/m} - a = u^n - a = 0$$

shows that $u^m$ is a root of $h$. If $h$ were reducible, then

$$h_1(x^m)h_2(x^m) = h(x^m) = x^n - a$$

shows that $x^n - a$ is reducible $\lightning$ hypothesis. Thus, $h$ is the irreducible polynomial of $u^m$, and

$$[K(u^m) : K] = \deg h = \tfrac{n}{m}$$

■

12. If $d \geqslant 0$ is an integer that is not a square, describe the field $\mathbb{Q}(\sqrt{d})$ and find a set of elements that generate the whole field.

$d$ is not a square $\implies$ $\sqrt{d} \notin \mathbb{Q}$, so the minimal polynomial of $d$ over $\mathbb{Q}$ is $f(x) = x^2 - d$. It is clear that $f$ is irreducible because it can only have factors of degree 1, and we know that $f$ factors linearly as $(x - d)(x + d)$ and neither factor is in $\mathbb{Q}[x]$. Then

$$\left[\mathbb{Q}(\sqrt{d}) : \mathbb{Q}\right] = \deg f = 2,$$

so $\{1, d\}$ is a basis for $\mathbb{Q}(\sqrt{d})$ over $\mathbb{Q}$. Thus,

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mathrel{\vdots} a, b \in \mathbb{Q}\}$$

■

13. Note: this was done in lecture, but not assigned.

a) Consider the extension $\mathbb{Q}(u)$ of $\mathbb{Q}$ generated by a real root of $f(x) = x^3 - 6x^2 + 9x + 3$. Express each of the following in terms of the basis $\{1, u, u^2\}$: $u^4, u^5$. To see that $f$ is irreducible over $\mathbb{Q}$, it suffices to show that $f$ is irreducible over $\mathbb{Z}$, by III.6.13. But $f$ is irreducible over $\mathbb{Z}$, by Eisenstein's Criterion with $p = 3$. Now $u^3 = 6u^2 - 9u - 3$ by construction, so

$$\begin{aligned} u^4 &= 6u^3 - 9u^2 - 3u \\ &= 6\left(6u^2 - 9u - 3\right) - 9u^2 - 3u \\ &= 36u^2 - 45u - 18 - 9u^2 - 3u \\ &= 27u^2 - 48u - 18 \end{aligned}$$

Then

$$\begin{aligned} u^5 &= 27u^3 - 48u^2 - 18u \\ &= 27\left(6u^2 - 9u - 3\right) - 48u^2 - 18u \\ &= 162u^2 - 243u - 81 - 48u^2 - 18u \\ &= 114u^2 - 261u - 81 \end{aligned}$$

14. Note: this was done in lecture, but not assigned.

a) If $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, find $[F : \mathbb{Q}]$ and a basis of $F$ over $\mathbb{Q}$.

The irreducible polynomial of $\sqrt{3}$ over $\mathbb{Q}$ is $x^2-3$, so $\left[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}\right] = 2$. Then the irreducible polynomial of $\sqrt{2}$ over $\mathbb{Q}(\sqrt{3})$ is $x^{-}2$, so $\left[Q(\sqrt{2}, \sqrt{3}) : Q(\sqrt{3})\right] = 2$. To see that $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$, suppose it were: then $\sqrt{2} = a+b\sqrt{3}$, for some $a, b \in \mathbb{Q}$. Then

$$\sqrt{2} = a + b\sqrt{3} \Rightarrow 2 = a^2 + 2b\sqrt{3} + 3b^2,$$

which is clearly impossible. Hence,

$$\left[Q(\sqrt{2}, \sqrt{3}) : Q\right] = \left[Q(\sqrt{2}, \sqrt{3}) : Q(\sqrt{3})\right] \cdot \left[Q(\sqrt{3}) : Q\right] = 2 \cdot 2 = 4$$

b) If $F = \mathbb{Q}(i, \sqrt{3}, \omega)$, where $i = \sqrt{-1}$ and $\omega$ is a nonreal cube root of 1, find $[F : \mathbb{Q}]$ and a basis of $F$ over $\mathbb{Q}$.

$i$ has irreducible polynomial $x^2+1$ over $\mathbb{Q}$, so $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. Then the irreducible polynomial of $\sqrt{3}$ over $\mathbb{Q}(i)$ is $x^2 - 3 \in \mathbb{Q}(i)[x]$, so

$$\left[\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}(i)\right] = \left[\mathbb{Q}(i, \sqrt{3}) : \mathbb{Q}(i)\right] \cdot [\mathbb{Q}(i) : \mathbb{Q}] = 2 \cdot 2 = 4$$

Since $i$ and $\sqrt{3}$ are linearly independent, $\left\{1, i, \sqrt{3}\right\}$ is a basis of $\mathbb{Q}(i, \sqrt{3})$ over $\mathbb{Q}$. Now notice that $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2} i \in \mathbb{Q}(i, \sqrt{3})$, so $\mathbb{Q}(i, \sqrt{3}, \omega) = \mathbb{Q}(i, \sqrt{3})$.

15. In the field $K(x)$, let $u = \frac{x^3}{x+1}$. Show that $K(x)$ is a simple extension of the field $K(u)$. What is $[K(x) : K(u)]$?

Let

$$f(y) = y^3 - \tfrac{x^3}{x+1}(y+1) = y^3 - \tfrac{x^3}{x+1} y - \tfrac{x^3}{x+1} \in K(u)[y]$$

so that $x$ is a root of $f$. Then $f$ is irreducible by Eisenstein's Criterion, with $p = \frac{x^3}{x+1} \in K(u)$. Then

$$[K(x) : K(u)] = \deg f = 3$$

and $\{1, x, x^2\}$ is a basis of $K(x)$ over $K(u)$. Also note that

$$K(x) = K(x, \tfrac{x^3}{x+1}) = K\left(\tfrac{x^3}{x+1}\right)(x),$$

so $K(x)$ is a simple extension of $K(u)$. ■

17. Find an irreducible polynomial $f$ of degree 2 over the field $\mathbb{Z}_2$? Adjoin a root $u$ of $f$ to $\mathbb{Z}_2$ to obtain a field $\mathbb{Z}_2(u)$ of order 4. Use the same method to construct a field of order 8.

Let $u$ be a root of $f(x) = x^2 + x + 1$[1]. $f$ is irreducible because $f(0) = 1$ and $f(1) = 3 \equiv_2 1$, so $f$ has no linear factors in $\mathbb{Z}_2[x]$. Hence, $\mathbb{Z}_2(u) = \{0, 1, u, 1 + u\}$.

| $+$ | $0$ | $1$ | $u$ | $1+u$ |
|---|---|---|---|---|
| $0$ | $0$ | $1$ | $u$ | $1+u$ |
| $1$ | $1$ | $0$ | $1+u$ | $u$ |
| $u$ | $u$ | $1+u$ | $0$ | $1$ |
| $1+u$ | $1+u$ | $u$ | $1$ | $0$ |

| $\times$ | $0$ | $1$ | $u$ | $1+u$ |
|---|---|---|---|---|
| $0$ | $0$ | $0$ | $0$ | $0$ |
| $1$ | $0$ | $1$ | $u$ | $1+u$ |
| $u$ | $0$ | $u$ | $1+u$ | $1$ |
| $1+u$ | $0$ | $1+u$ | $1$ | $u$ |

To construct a field of order 8, we need to adjoin the root of an irreducible cubic. Define $g(x) = x^3 + x + 1$. Then $g$ is irreducible because $g(0) = 1$ and $g(1) = 3 \equiv_2 1$, so $g$ has no linear factors in $\mathbb{Z}_2[x]$.

[1]This polynomial was found by trial and error / exhaustion

22. F is an algebraic $\iff$ for every intermediate field $E$, every monomorphism $\sigma : E \to E$ which is the identity on $K$ is in fact an automorphism of $E$.

$\boxed{\Rightarrow}$ Let $E$ be an intermediate field of the extension $F : K$, and let $\sigma : E \to E$ be a monomorphism fixing $K$. We need to show that $\sigma$ is surjective, so pick $u \in E \backslash K$ and find its preimage under $\sigma$. Since $F : K$ is algebraic and $u \in E \subset F$, $u$ must be algebraic over $K$. Then let $f$ be the irreducible polynomial of $u$. Now $f(u) = \sum_{i=0}^{n} a_i u^i = 0$ implies that

$$\begin{aligned} \sigma f(u) &= \sigma\left(\sum\nolimits_{i=0}^{n} a_i u^i\right) \\ &= \sum\nolimits_{i=0}^{n} \sigma\left(a_i u^i\right) \\ &= \sum\nolimits_{i=0}^{n} \sigma\left(a_i\right) \sigma\left(u^i\right) \\ &= \sum\nolimits_{i=0}^{n} a_i \sigma\left(u\right)^i \\ &= 0, \end{aligned}$$

showing that $\sigma(u)$ is also a root of $f$, by the ring-homomorphism properties of $\sigma$. Since $f$ can only have finitely many roots,

$$\left| \left\{ \sigma^k\left(u\right) \vdots\, k \in N \right\} \right| = n < \infty.$$

Since $\sigma : E \to E$, we know $\sigma^k(u) \in E, \forall k$. Hence, $\sigma^{n-1}(u) \in E$. Then

$$\sigma\left(\sigma^{n-1}\left(u\right)\right) = \sigma^n\left(u\right) = u$$

shows that $\sigma^{n-1}(u)$ is in the preimage of $u$. Since this is true for any $u \in E$, $\sigma$ must be surjective.

$\boxed{\Leftarrow}$ Strategy: suppose $F : K$ is not algebraic and find a $\sigma$ which is not surjective.

If $F : K$ is transcendental, then there is some $u \in F \backslash K$ which is not the root of any polynomial in $K[x]$. $K(u)$ has basis $\{1, u, u^2, \ldots\}$ over $K$, so the action of any $\sigma$ fixing $K$ is completely determined by its action on $u$[2]. Define $\sigma : K(u) \to K(u)$ by $\sigma(u) = u^2$. Then $u$ can have no preimage under $\sigma$. If it did, then $\exists v \in K(u)$ such that $\sigma(v) = u$. Then

$$v = a_0 + a_1 u + \ldots + a_n u^n = \sum\nolimits_{i=0}^{n} a_i u^i,\ a_i \in K$$

because $v \in K(u)$. Also,

$$\sigma(v) = \sum\nolimits_{i=0}^{n} \sigma\left(a_i u^i\right) = \sum\nolimits_{i=0}^{n} a_i \sigma(u)^i = \sum\nolimits_{i=0}^{n} a_i u^{2i}$$

But this would imply that $u$ is a root of

$$f(x) = \left(\sum\nolimits_{i=0}^{n} a_i x^{2i}\right) - x \in K[x]$$

$\lightning$ $u$ is transcendental.

[2]All other $u^i$ will be determined by the image of $u$ under $\sigma$: $\sigma(u^i) = \sigma^i(u)$

Alternative $\boxed{\Leftarrow}$ proof for 23: Pick $u \in E$, where $E$ is any intermediate field of the extension $F : K$. Let $\sigma : K \xrightarrow{id} K$ be the identity. Then we can extend this to a homomorphism $\sigma : K(u) \longrightarrow K(u)$ by defining $\sigma(\frac{f(u)}{g(u)}) = \frac{f(u^2)}{g(u^2)}$ for any element $v = \frac{f(u)}{g(u)} \in E \backslash K$. Now

$$\sigma\left(\frac{f_1(u)}{g_1(u)} + \frac{f_2(u)}{g_2(u)}\right) = \sigma\left(\frac{f_1(u)g_2(u)+f_2(u)g_1(u)}{g_1(u)g_2(u)}\right) = \frac{f_1(u^2)g_2(u^2)+f_2(u^2)g_1(u^2)}{g_1(u^2)g_2(u^2)}$$

$$\sigma\left(\frac{f_1(u)}{g_1(u)}\right) + \sigma\left(\frac{f_2(u)}{g_2(u)}\right) = \frac{f_1(u^2)}{g_1(u^2)} + \frac{f_2(u^2)}{g_2(u^2)} = \frac{f_1(u^2)g_2(u^2)+f_2(u^2)g_1(u^2)}{g_1(u^2)g_2(u^2)}$$

$$\sigma\left(\frac{f_1(u)f_2(u)}{g_1(u)g_2(u)}\right) = \frac{f_1(u^2)f_2(u^2)}{g_1(u^2)g_2(u^2)} = \frac{f_1(u^2)}{g_1(u^2)} \cdot \frac{f_2(u^2)}{g_2(u^2)} = \sigma\left(\frac{f_1(u)}{g_1(u)}\right) \cdot \sigma\left(\frac{f_2(u)}{g_2(u)}\right)$$

shows that $\sigma$ is a homomorphism.

case i) $\sigma$ is not injective. Then $\exists \frac{f(u)}{g(u)} \in \ker \sigma$, i.e., $\sigma\left(\frac{f(u)}{g(u)}\right) = 0$, where $f(u) \neq 0$. So $f(u^2) = 0$ shows that $u$ is algebraic over $K$.

case ii) $\sigma$ is injective. Then the hypotheses give that $\sigma$ is also surjective, so there is some $\frac{f(u)}{g(u)} \in E$ such that $\sigma\left(\frac{f(u)}{g(u)}\right) = \frac{f(u^2)}{g(u^2)} = u$. Then $f(u^2) - ug(u^2) = 0$ shows that $u$ is algebraic over $K$, because $u$ is a root of

$$h(x) = f(x^2) - xg(x^2) \in K[x].$$

$\blacksquare$

23. If $u \in F$ is algebraic over $K(U)$ for some $U \subset F$, then there exists a finite subset $U' \subset U$ such that $u$ is algebraic over $U'$.

If $u$ is algebraic over $K(U)$, then $u$ is the root of some irreducible polynomial

$$\begin{aligned}\varphi(x) &= \sum_{i=0}^{n} \frac{f_i(u_1,\ldots,u_m)}{g_i(u_1,\ldots,u_m)} x^i \\ &= \frac{f_0(u_1,\ldots,u_m)}{g_0(u_1,\ldots,u_m)} + \frac{f_1(u_1,\ldots,u_m)}{g_1(u_1,\ldots,u_m)} x + \ldots + \frac{f_n(u_1,\ldots,u_m)}{g_n(u_1,\ldots,u_m)} x^n \in K\left(U\right)[x]\end{aligned}$$

Let $U' = \{u_1, \ldots, u_m\}$. Then $U'$ is clearly finite, and $u$ is algebraic over $K(U')$ by construction.