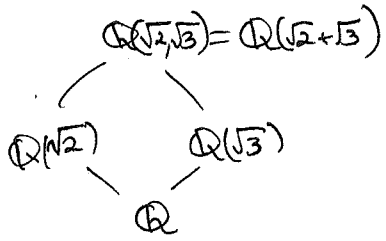
§15.8 The primitive element theorem

Recall we saw $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$:



($\alpha = \sqrt{2}$, $\beta = \sqrt{3}$, $\gamma = \sqrt{2}+\sqrt{3}$)

This always happens in characteristic 0 (and for finite fields; see EXER 15.8.1).

THEOREM (15.8.1): When $\mathrm{char}(\mathbb{F}) = 0$, any finite extension $\mathbb{K} \supset \mathbb{F}$ ($[\mathbb{K}:\mathbb{F}] < \infty$) has $\mathbb{K} = \mathbb{F}(\gamma)$ for some $\gamma \in \mathbb{K}$.
(γ called a primitive element for $\mathbb{K}$ over $\mathbb{F}$.)

proof: Since $[\mathbb{K}:\mathbb{F}]$ finite implies $\mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_r)$ for some α_i algebraic over $\mathbb{F}$, using induction on r, it suffices to prove $\mathbb{F}(\alpha,\beta) = \mathbb{F}(\gamma)$ when α, β are algebraic over $\mathbb{F}$: then $\mathbb{K} = \underbrace{\mathbb{F}(\alpha_1,\ldots,\alpha_{r-1})}_{=\mathbb{F}(\hat{\gamma})}(\alpha_r) = \mathbb{F}(\hat{\gamma},\alpha_r) = \mathbb{F}(\gamma)$
($\hat{\gamma}$ by induction)

So given α, β algebraic over $\mathbb{F}$, pick an extension $\mathbb{K} \supset \mathbb{F}$ so that

$$f(x) = m_{\mathbb{F},\alpha}(x) = (x-\overset{\alpha}{\alpha_1})(x-\alpha_2)\cdots(x-\alpha_m)$$
$$g(x) = m_{\mathbb{F},\beta}(x) = (x-\underset{\beta}{\beta_1})(x-\beta_2)\cdots(x-\beta_n)$$

(i.e. $\mathbb{K}$ splits $f(x)g(x)$)

Note $\alpha_1, \ldots, \alpha_m$ are distinct,
$\beta_1, \ldots, \beta_n$ are distinct (why?)

We claim that if we pick $c \in \mathbb{F}$ so that

$$\boxed{\beta_j + c\alpha_i \neq \beta_k + c\alpha_\ell \quad \text{for } (i,j) \neq (\ell,k)}$$

i.e. $c(\alpha_i - \alpha_\ell) \neq \beta_k - \beta_j$ if $i \neq \ell$

$$c \neq \frac{\beta_k - \beta_j}{\alpha_i - \alpha_\ell}$$

Q: Why can we pick such a $c \in \mathbb{F}$?

A: Can avoid these finitely many bad values

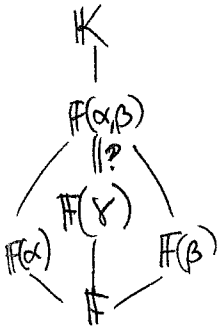
then $\gamma = \beta_1 + c\alpha_1$ has $\mathbb{F}(\alpha,\beta) = \mathbb{F}(\gamma)$
$= \beta + c\alpha$

(80)
4/3/2019 To see this, it's enough to show $\alpha_1 = \alpha \in F(\gamma)$ since then also $\beta_1 = \gamma - c\alpha_1 \in F(\gamma)$.

We'll show $x - \alpha_1 = \gcd_{F(\gamma)[x]}\big(f(x), g(\gamma - cx)\big)$ $\big(\in F(\gamma)[x] \Rightarrow \alpha \in F(\gamma)\big)$

α_1 is a root of this i.e. $f(\alpha_1) = 0$

$g(\gamma - c\alpha_1) = g(\beta_1) = 0$, so α_1 is also a root of this



$= \gcd_{K[x]}\big(f(x), g(\gamma - cx)\big)$

$f(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$

$\alpha_2, \ldots, \alpha_n$ are not roots of this, since this would require

$\gamma - c\alpha_i = \beta_j$ for some $i = 2, \ldots, n$

$(\beta_1 + c\alpha_1) - c\alpha_i = \beta_j$

$\beta_1 + c\alpha_1 = \beta_j + c\alpha_i$

Contradiction to our choice of c.

∎

Chapter 16 Galois Theory

We'll understand how looking at field extensions $\mathbb{F} \subset \mathbb{K}$ and the group $G(\mathbb{K}/\mathbb{F}) = \{ \text{all } \mathbb{F}\text{-automorphisms } \mathbb{K} \xrightarrow{\sigma} \mathbb{K} \}$ (sometimes called $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$ or $\mathrm{Aut}_{\mathbb{F}}(\mathbb{K})$ or $\mathrm{Gal}(\mathbb{K},\mathbb{F})$)

$\mathbb{F} \subset \mathbb{K}$ fixed by σ

can help us understand more, including the lack of a quintic formula.

§16.3, 16.4 Splitting fields (maybe we'll come back to §16.1, 2)

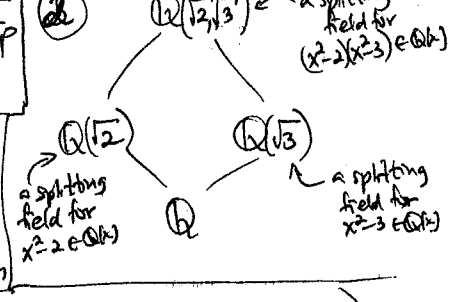
DEF'N: Say that $\mathbb{F} \subset \mathbb{K}$ and $f(x) \in \mathbb{F}[x]$ have $\mathbb{K}$ being a splitting field for $f(x)$ over $\mathbb{F}$ if

- "$\mathbb{K}$ is not too small" • $f(x)$ splits completely in $\mathbb{K}$ i.e. $f(x) = c\prod_{i=1}^{n}(x-\alpha_i)$, $\alpha_i \in \mathbb{K}$
- "$\mathbb{K}$ is not too big" • $\mathbb{K} = \mathbb{F}(\alpha_1, \dots, \alpha_n)$

EXAMPLES: ① $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) \subset \mathbb{C}$, with $\omega = e^{2\pi i/3}$

$\mathbb{F}$ = $\mathbb{Q}$; $\mathbb{Q}(\sqrt[3]{2})$ too small; $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$ is a splitting field for $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$; $\mathbb{C}$ too big

③ $\mathbb{F}_{p^d}$ is a splitting field for $f(x) = x^{p^d} - x$ over $\mathbb{F}_p$

② 

Splitting fields have some remarkable properties

- they're ~~existential~~ unique up to isomorphism
- they split more than you'd expect! (irreducibles having one root in a splitting field means they'll have all of them (?))

They exist, of course, since we can always split $f(x) \in \mathbb{F}[x]$ in some extension $\mathbb{K}' \supset \mathbb{F}$ and then let $\mathbb{K} := \mathbb{F}(\alpha_1, \dots, \alpha_n)$ where $\alpha_1, \dots, \alpha_n$ are the roots of $f(x)$ inside $\mathbb{K}'$

PROPOSITION: (16.4.3 (b) + more) Given a field isomorphism $F_1 \xrightarrow{\varphi} F_2$ and two polynomials $f_1(x) \in F_1[x]$ with $\varphi(f_1) = f_2$, $f_2(x) \in F_2[x]$, then one can extend φ to an isomorphism $K_1 \xrightarrow{\tilde{\varphi}} K_2$ between any splitting fields K_1 for f_1 and K_2 for f_2.

$$\begin{array}{ccc} K_1 & \xrightarrow{\tilde{\varphi}} & K_2 \\ \cup & & \cup \\ F_1 & \xrightarrow{\varphi} & F_2 \end{array}$$

REMARK: our proof will show, in fact, we can make $\tilde{\varphi}$ take any root α_1 of f_1 with $m_{F_1,\alpha_1}(x)$ as min. poly to any root α_2 of $\varphi(m_{F_1,\alpha_1}(x))$

COR: In particular, any two splitting fields K_1, K_2 for $f(x) \in F[x]$ are F-isomorphic:

$$\begin{array}{ccc} K_1 & \xrightarrow{\tilde{\varphi}} & K_2 \\ \cup & & \cup \\ F & \xrightarrow[\mathrm{id}_F = \varphi]{} & F \end{array}$$

(So it is fair to call any of them $\mathrm{split}_F(f(x)) =: K$)

4/5/2019>

proof: Induct on $[K_1 : F_1]$. (not the proof in Artin!)

BASE CASE $[K_1 : F_1] = 1$ has $K_1 = F_1$, so $f_1(x)$ splits in F_1 $c\prod_{i=1}^{n}(x-\alpha_i)$, $\alpha_i \in F_1$

and then $f_2(x) = \varphi(f_1(x))$ splits in $F_2 = K_2$,

$$= \varphi(c)\prod_{i=1}^{n}(x-\varphi(\alpha_i))$$

so $\tilde{\varphi} = \varphi$ works.

In the INDUCTIVE STEP, pick an irreducible factor $g_1(x)$ of $f_1(x)$ in $F_1[x]$ so that $g_2(x) = \varphi(g_1)$ is an irred factor of $f_2(x)$ in $F_2[x]$.

Letting α_1 be a root of $g_1(x)$ (and $f_1(x)$) in K_1 then $\alpha_2 = \varphi(\alpha_1)$ is a root of $g_2(x)$ (and $f_2(x)$) in K_2.

We can extend φ like this:

$$\begin{array}{ccccc} K_1 & & \cdots \exists \tilde{\varphi} \cdots & & K_2 \\ \cup & & & & \cup \\ F_1(\alpha_1) \cong & F_1[x]/g_1(x) & \xrightarrow{\varphi} & F_2[x]/g_2(x) & \cong F_2(\alpha_2) \\ \cup & & & & \cup \\ F_1 & & \xrightarrow{\qquad\varphi\qquad} & & F_2 \end{array}$$

Now replace F_1, F_2 with $F_1(\alpha_1), F_2(\alpha_2)$, and apply induction. ∎