



# Fields

Book II

Eq.  $\alpha = \sqrt{2+\sqrt{2}}$   
 $\alpha^2 = 2+\sqrt{2}$   
 $\alpha^2 - 2 = \sqrt{2}$   
 $\alpha^4 - 4\alpha^2 + 4 = 2$   
 $\alpha^4 - 4\alpha^2 + 2 = 0$

The minimal poly. of  $\alpha$  over  $\mathbb{Q}$  is  $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$ .  
 (Exercise:  $f(x)$  is irreducible in  $\mathbb{Q}[x]$  so it really is the min. poly. of  $\alpha$  over  $\mathbb{Q}$ )  
 The roots of  $f(x)$  are

$\alpha = \sqrt{2+\sqrt{2}}$   
 $-\alpha = -\sqrt{2+\sqrt{2}}$   
 $\beta = \sqrt{2-\sqrt{2}}$   
 $-\beta = -\sqrt{2-\sqrt{2}}$

$f(x) = x^4 - 4x^2 + 2 = (x-\alpha)(x+\alpha)(x-\beta)(x+\beta)$

In this case  $E = \mathbb{Q}[\alpha] = \{a + b\alpha + c\alpha^2 + d\alpha^3 : a, b, c, d \in \mathbb{Q}\}$  contains all the roots of  $f(x)$  so it is a normal extension of  $\mathbb{Q}$ .

$\beta = \sqrt{2+\sqrt{2}} \sqrt{2-\sqrt{2}} = \sqrt{4-2} = \sqrt{2} = \alpha^2 - 2$

$\beta = (*) + (*)\alpha + (*)\alpha^2 + (*)\alpha^3 = \alpha^3 - 3\alpha$

$\Rightarrow \beta = \frac{\alpha^3 - 2}{\alpha} \in \mathbb{Q}(\alpha) = \mathbb{Q}[\alpha]$

$\alpha^4 - 4\alpha^2 + 2 = 0$

$\alpha^3 - 4\alpha + \frac{2}{\alpha} = 0 \Rightarrow \frac{2}{\alpha} = 4\alpha - \alpha^3$

$\alpha^4 = 4\alpha^2 - 2$

$\alpha^6 = 4\alpha^4 - 2\alpha^2 = 4(4\alpha^2 - 2) - 2\alpha^2 = 14\alpha^2 - 8$

Look for an automorphism  $\sigma: E \rightarrow E$  ( $E = \mathbb{Q}[\alpha]$ ) satisfying  $\sigma(\alpha) = \beta$ .

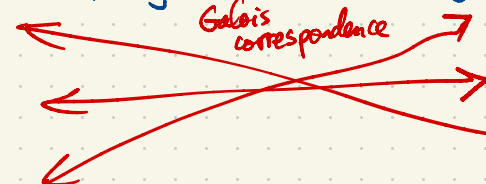
$\sigma(\beta) = \sigma(\alpha^3 - 3\alpha) = \sigma(\alpha)^3 - 3\sigma(\alpha) = \beta^3 - 3\beta = (\alpha^3 - 3\alpha)^3 - 3(\alpha^3 - 3\alpha) = (\alpha^3 - 3\alpha)(\alpha^3 - 3\alpha - 3)$   
 $= (\alpha^3 - 3\alpha)(\alpha^6 - 6\alpha^4 + 9\alpha^2 - 3) = (\alpha^3 - 3\alpha)(14\alpha^2 - 8 - 6(4\alpha^2 - 2) + 9\alpha^2 - 3) = (\alpha^3 - 3\alpha)(-\alpha^2 + 1) = \alpha(\alpha^2 - 3)(-\alpha^2 + 1)$   
 $= \alpha(-\alpha^4 + 4\alpha^2 - 3) = \alpha(-4\alpha^2 + 2 + 4\alpha^2 - 3) = -\alpha$

$\sigma: \alpha \mapsto \beta = \alpha^3 - 3\alpha \mapsto -\alpha \mapsto -\beta \mapsto \alpha$

Aut  $E = \langle \sigma \rangle$  of order 4; cyclic.

$G = \text{Aut } E = \langle \sigma \rangle = \{1, \sigma, \sigma^2, \sigma^3\}$

$\mathbb{Q}[\alpha]$   
 $\downarrow$   
 $\mathbb{Q}[\sqrt{2}]$   
 $\downarrow$   
 $\mathbb{Q}$



$\langle \sigma^2 \rangle = \{1, \sigma^2\}$   
 $\langle \sigma \rangle = \{1, \sigma, \sigma^2, \sigma^3\}$

$\sigma(\sqrt{2}) = ?$   
 $\sqrt{2} = \alpha\beta$   
 $\sigma(\sqrt{2}) = \sigma(\alpha)\sigma(\beta) = \beta(-\alpha) = -\alpha\beta = -\sqrt{2}$   
 $\sigma(\alpha) = \beta$   
 $\sigma(-\alpha) = -\sigma(\alpha) = -\beta$   
 $\sigma(\beta) = -\alpha$   
 $\sigma(-\beta) = -\sigma(\beta) = \alpha$   
 $\sigma(\sqrt{2}) = \sigma(\alpha^2 - 2) = \sigma(\alpha)^2 - 2 = \beta^2 - 2 = -\sqrt{2}$   
 $= \sigma(-\sqrt{2}) = \sqrt{2}$