Notes on Bi-Quadratic Extensions

Ken Lee

Spring 2021

Proposition – Classification of Bi-Quadratic Extensions
Let $a, b \in K$ a field of characteristic not 2 and b non-square in K. Let $K \to L$ be a splitting field of $(X^2 - a)^2 - b$. The roots are then $\pm\sqrt{a \pm \sqrt{b}}$ and we have the tower,

$$\begin{tikzcd} & & K(\sqrt{a+\sqrt{b}}) \arrow[dr] & \\ K \arrow[r, "2"] & K(\sqrt{b}) \arrow[ur] \arrow[dr] & & L \\ & & K(\sqrt{a-\sqrt{b}}) \arrow[ur] & \end{tikzcd}$$

Define the mysterious $c := a^2 - b$. Then the following are true :

1. Let c be a square in K. Then we have cases :
   (a) Let either $2(a + \sqrt{c}), 2(a - \sqrt{c})$ square in K. (We cannot have both since b non-square in K.) Then $L = K(\sqrt{b})$ and hence $\mathrm{Aut}_K L \cong C_2$.
   (b) Let both $2(a \pm \sqrt{c})$ non-squares in K. Then $[L : K] = 4$ and $\mathrm{Aut}_K L \cong C_2 \times C_2$.
2. Let c non-square in K. Then we have cases :
   (a) Let bc square in K. Then $[L : K] = 4$ and $\mathrm{Aut}_K L \cong C_4$.
   (b) Let bc non-square in K. Then $[L : K] = 8$ and $\mathrm{Aut}_K L \cong D_{2(4)}$.

Proof. Throughout the proof, we use α, α' to denote $\sqrt{a+\sqrt{b}}, \sqrt{a-\sqrt{b}}$ respectively. We first give an ansatz of what $\sigma \in \mathrm{Aut}_K L$ could do by exploiting $\mathrm{Aut}_K L \hookrightarrow \mathrm{Aut}\,\{\pm\alpha, \pm\alpha'\}$. Let $\sigma \in \mathrm{Aut}_K L$ which we view as a subgroup of the permutations of the roots. We have the cases :

- $\sigma(\alpha) = \alpha$. Then $\sigma(-\alpha) = -\alpha$. So we have two cases :
  - $\sigma = \mathbb{1}$
  - $\sigma = (\alpha' \ -\alpha')$, a reflection.

- $\sigma(\alpha) = \alpha'$. Then $\sigma(-\alpha) = -\alpha'$. So we have two cases :
  - $\sigma = (\alpha\ \alpha')(-\alpha\ -\alpha')$, a diagonal reflection.
  - $\sigma = (\alpha\ \alpha'\ -\alpha\ -\alpha')$.
- $\sigma(\alpha) = -\alpha$. Then we have either :
  - $\sigma = (\alpha\ -\alpha)$, a reflection.
  - $\sigma = (\alpha\ -\alpha)(\alpha'\ -\alpha') = (\alpha\ \alpha'\ -\alpha\ -\alpha')^2$.
- $\sigma(\alpha) = -\alpha'$. Then either :
  - $\sigma = (\alpha\ -\alpha')(-\alpha\ \alpha')$, a diagonal reflection.
  - $\sigma = (\alpha\ -\alpha'\ -\alpha\ \alpha') = (\alpha\ \alpha'\ -\alpha\ -\alpha')^{-1}$

So we see $\mathrm{Aut}_K L \cong D_{2(4)}$ when its cardinality is largest, otherwise we obtain subgroups of $D_{2(4)}$.

The Galois group $\mathrm{Aut}_K L$ depends crucially on two things :

(Q1) Are $K(\sqrt{b}) \to K(\alpha)$, $K(\sqrt{b}) \to K(\alpha')$ trivial?

(Q2) Is $K(\alpha) = K(\alpha')$?

Considering (Q1), let $a \pm \sqrt{b}$ is a square in $K(\sqrt{b})$. Then we have $x, y \in K$ such that

$$\begin{aligned} a \pm \sqrt{b} = (x + y\sqrt{b})^2 = x^2 + by^2 + 2xy\sqrt{b} &\Rightarrow a = x^2 + b\left(\frac{\pm 1}{2x}\right)^2 \\ \Rightarrow 0 = x^4 - ax^2 + b/4 &\Rightarrow x^2 = \frac{a \pm \sqrt{c}}{2} \end{aligned}$$

where $c := a^2 - b$, the discriminant of the quadratic in x^2, which is not so mysterious afterall.

(*Assume c square in* K) (*One of* $2(a \pm \sqrt{c})$ *square in* K) Suppose $2(a + \sqrt{c})$ square in K. Then $K(\alpha) = K(\sqrt{b})$. Since $\alpha\alpha' = \sqrt{c} \in K$, we hence have $L = K(\alpha, \alpha') = K(\sqrt{b})$. As for the Galois group, since $[L : K] = 2$, we cannot have any 4-cycles in $\mathrm{Aut}_K L$. This leaves the identity, the reflections and $(\alpha\ -\alpha)(\alpha'\ -\alpha')$. Any automorphism fixing $\sqrt{b}$ or α or α' must be identity since $L = K(\sqrt{b}) = K(\alpha) = K(\alpha')$. This leaves the identity and two reflections diagonal reflections. Finally, which reflection is in $\mathrm{Aut}_K L$ hinges on which of $\alpha + \alpha'$ or $\alpha - \alpha'$ is in K. This is the other significance of $2(a + \sqrt{c})$: $(\alpha + \alpha')^2 = 2(a + \sqrt{c})$. So by assumption $\alpha + \alpha' \in K$. Now if $(\alpha\ -\alpha')(\alpha'\ -\alpha) \in \mathrm{Aut}_K L$, we would have $\alpha - \alpha' \in K$ and hence $\alpha \in K$, a contradiction. Thus, $\mathrm{Aut}_K L$ is generated by $(\alpha\ \alpha')(-\alpha\ -\alpha')$.

The above argument can be repeated instead with assuming $2(a - \sqrt{c})$ is a square in K. Then everything is the same until the last step, where we find $\mathrm{Aut}_K L$ is generated by $(\alpha\ -\alpha')(-\alpha\ \alpha')$ instead.

(*Both* $2(a \pm \sqrt{c})$ *non-square in* K) Both $a \pm \sqrt{b}$ are not squares in $K(\sqrt{b})$, so $K(\sqrt{b}) \to K(\alpha), K(\sqrt{b}) \to K(\alpha')$ are both degree 2. But again $\alpha\alpha' = \sqrt{c} \in K$, so $L = K(\alpha, \alpha') = K(\alpha) = K(\alpha')$ and hence $[L : K] = 4$. Any automorphism fixing α or α' must be identity, so this excludes the non-diagonal reflections. Since $(\alpha \pm \alpha')^2 = 2(a \pm \sqrt{c})$, we have at least three sub-K-extensions $K(\sqrt{b}), K(\alpha \pm \alpha')$. By Galois theory, this gives at least three subgroups of $\mathrm{Aut}_K L$ with index 2. It thus cannot be the case that $\mathrm{Aut}_K L$ is generated by the 4-cycles, and hence $\mathrm{Aut}_K L$ is generated by the diagonal reflections, isomorphic to V_4.

(c *non-square in* K) The extensions $K(\sqrt{b}) \to K(\alpha), K(\sqrt{b}) \to K(\alpha')$ must be order 2. The question is $(Q2)$. After thinking for a while, a thing one might try is the following :

> *Lemma. Let F be a field with non-even characteristic. Let $r, s \in F$ with s non-square in F. Then $\sqrt{r} \in F(\sqrt{s})$ if and only if rs or r is a square in F.*
>
> *Proof.* ($\Rightarrow$) Let $r = (x + y\sqrt{s})^2$ with $x, y \in F$. We get $r = x^2 + sy^2$ and $0 = 2xy$. So either $r = x^2$ or $rs = (sy)^2$.
>
> ($\Leftarrow$) $r = x^2/s = (x/\sqrt{s})^2$. ■

So we have $\alpha' \in K(\alpha) = K(\sqrt{b})(\alpha)$ if and only if $c = \alpha\alpha'$ or $a - \sqrt{b}$ square in $K(\sqrt{b})$. The latter implies $(a - \sqrt{c})/2$ is a square in K and hence $\sqrt{c} \in K$, a contradiction. So $K(\alpha') = K(\alpha)$ if and only if c is a square in $K(\sqrt{b})$. But this is if and only if $\sqrt{c} \in K(\sqrt{b})$, which by another application of the lemma, is equivalent to bc or c being a square in K. The latter is again false by assumption, so we have $K(\alpha) = K(\alpha')$ if and only if bc is a square in K.

(bc *is a square in* K) We have $L = K(\alpha) = K(\alpha')$ and $[L : K] = 4$. Again, any automorphism fixing α or α' must be identity so we are left with the rotations and the diagonal reflections. If $\mathrm{Aut}_K L$ is generated by the diagonal reflections, then $[K(\alpha \pm \alpha') : K]$ would be order two and hence $\min(\alpha \pm \alpha', K) = X^2 - 2(a \pm \sqrt{c})$, in particular $\sqrt{c} \in K$, a contradiction. So $\mathrm{Aut}_K L$ is generated by a 4-cycle.

(bc *is non-square in* K) Covered. □