MATH5725 Galois Theory (S2, 2014)

Lecture 1

Problem: compute intermediate fields of a bi-quadratic field
Let $A, B \in \mathbf{Q}$ (or k, so long as k is not of characteristic 2), so that AB is not a square. We want to determine all the subfields of $K = \mathbf{Q}(\sqrt{A}, \sqrt{B})$. First observations are:
1. if $L \subset K$ then $[L : \mathbf{Q}] \mid 4$, because of:

Proposition 1. *If $K/L/k$ is a tower of finite[1] field extensions then:*

$$[K : L][L : k] = [K : k].$$

Proof. Recall that the degree $[K : L]$ is the dimension of K as an L-vectorspace.
We proceed by the following argument: let $\alpha_1, \cdots, \alpha_m$ be a basis for for L as an k vector space, and let $\beta_1, \cdots, \beta_n$ be a basis for K as an L vector space. Then $\alpha_i\beta_j$ is an element of K (because K is a field) and is a basis for K as an k vector space.
To be careful we need to check it really is a basis, which means checking that: 1) all elements of K can be written as a linear combination of the $\alpha_i\beta_j$, and 2) the linear combination is unique, or equivalently, zero can only be represented as zero. Both 1) and 2) follow as if $\lambda \in K$ then

$$\lambda = \sum_i a_i\alpha_i = \sum_i (\sum_j b_j\beta_j)\alpha_i = \sum_{ij} b_j\alpha_i\beta_j$$

so 1 follows, and 2 follows as $\lambda = 0$ imples that $a_i = 0$ (as α_i is a basis for K/L) and so $\sum b_j\beta_j = 0$ and $b_j = 0$ as β_j is a basis for K/k. □

2. So from the proposition $[L : K]$ is equal to $4, 2$ or 1. If it is 4 or 1 then either $L = \mathbf{Q}$ or $L = K$ (the reason is that if E/F is a field extension and E is a 1-dimensional F-vector space then $E = F.a$ and because $1 = \lambda a \in E$ with $\lambda \in F$ we have $a \in F$ - apply this to $L/\mathbf{Q}$ and K/L respectively).

3. There are 4 obvious subfields, namely $\mathbf{Q}, \mathbf{Q}(\sqrt{A}), \mathbf{Q}(\sqrt{B}), \mathbf{Q}(\sqrt{AB})$.
This leaves L/K quadratic. So L has basis $1, s$ with $s = a + b\sqrt{A} + c\sqrt{B} + d\sqrt{AB}$ and $s^2 = ts + v$ for some $t, v \in \mathbf{Q}$. Which gives a system of equations in a, b, c, d, t, v which need to be satisfied by expanding s^2 and $ts + v$ in terms of the basis for $\mathbf{Q}$ and comparing coefficients of basis elements. Namely:

$$\begin{aligned} s^2 &= a^2 + b^2A + c^2B + d^2AB + (2ab + 2cdB)\sqrt{A} + (2ab + 2bdA)\sqrt{B} + (2ad + 2bc)\sqrt{AB} \\ &= ts + v \\ &= ta + v + tb\sqrt{A} + tc\sqrt{B} + td\sqrt{AB} \end{aligned}$$

Trying to solve these equations would be tricky, time-consuming, and unpleasant, but doable, especially with a computer algebra system.

There's a better way: use group theory, divisibility properties of polynomials, and what is essentially, the Galois Correspondence (which we prove in this special case).

First, where does the group come from?

We define

$$\mathrm{Aut}(K/\mathbf{Q}) = \{\sigma : K \longrightarrow K \mid \sigma \text{ is a field automorphism and } \sigma(a) = a \text{ for all } a \in \mathbf{Q}\}.$$

This is known as the Galois group of the extension $\mathrm{Aut}(K/\mathbf{Q})$. It will also be written as $\mathrm{Gal}(K/\mathbf{Q})$.

[1] This was tacitly assumed in the lecture. It is true if K/L and L/k are infinite, but we do not need this case. The proof above can be adapted by letting α_i and β_j be indexed by infinite instead of finite sets and noting that only finitely many coefficients of the α_i and β_k will be non-zero so the sums make sense.

Now if $\sigma \in \mathrm{Aut}(K/\mathbf{Q})$, then $\sigma(\sqrt{A})^2 = \sigma(A) = A$, so $\sigma(\sqrt{A}) = \pm\sqrt{A}$; likewise $\sigma(\sqrt{B}) = \pm\sqrt{B}$. Moreover $\sigma(\sqrt{AB}) = \sigma(\sqrt{A})\sigma(\sqrt{B})$, and $\sigma(a + b\sqrt{A} + c\sqrt{B} + d\sqrt{AB}) = a + b\sigma(\sqrt{A}) + c\sigma(\sqrt{B}) + d\sigma(\sqrt{AB})$. From this we can conclude that σ is determined by and determines a pair $(\epsilon_1, \epsilon_2) \in \{\pm 1\}^2$ by the rule

$$\sigma \mapsto (\sqrt{A}/\sigma(\sqrt{A}), \sqrt{B}/\sigma(\sqrt{B})).$$

Moreover this map respects composition of automorphisms and so $\mathrm{Aut}(K/\mathbf{Q}) \cong \mathbf{Z}/2\times\mathbf{Z}/2$, the Klein four-group.

Now each of the fields we have written down is fixed by a specific element (and the subgroup generated by that element) of the Klein four-group, that is $\mathbf{Q}(\sqrt{A})$ is fixed by $(\pm 1, 1)$, $\mathbf{Q}(\sqrt{B})$ by $(1, \pm 1)$ and $\mathbf{Q}(\sqrt{AB})$ by $\pm(1, 1)$.[2] It turns out that all subfields are fixed by some subgroup of $\mathrm{Aut}(K/\mathbf{Q})$ and this is what we will prove. (Note in passing that it is no accident that $|\mathrm{Aut}(K/\mathbf{Q})| = [K : \mathbf{Q}]$.)

Indeed, from what we have written our subfield $L = \mathbf{Q}(s)$ is generated by 1-element (this is a special case of the so-called Primitive Element theorem). Moreover s satisfies a polynomial

$$X^2 - tX + v$$

which $\sigma(s)$ must also satisfy for $\sigma \in \mathrm{Aut}(K/\mathbf{Q})$ (because σ is a ring homomorphism). Therefore, since $P(\alpha) = 0$ implies $(X - \alpha) \mid P(X)$ we have

$$\prod_{\sigma\in\mathrm{Aut}(K/\mathbf{Q})} (X - \sigma(s)) \mid (X^2 - tX + v)^4.$$

Now

$$X^2 - tX + v = (X - s)(X - s').$$

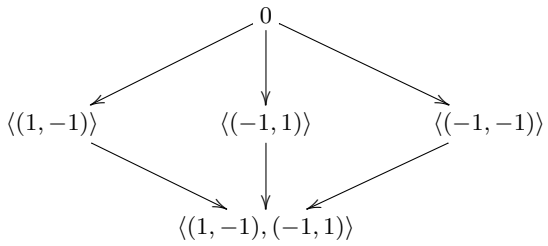
So since $\mathbf{Q}[X]$ is a unique factorisation domain, we have for some distinct $\sigma, \sigma' \in \mathrm{Aut}(K/\mathbf{Q})$ that $\sigma(s) = \sigma'(s)$ (by the Pigeon hole principle, since each $\sigma(s)$ is equal to either s or s'). In other words

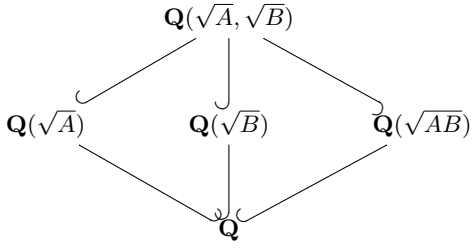
$$\sigma'^{-1} \circ \sigma(s) = s$$

and so s is invariant under the group generated by $\sigma'^{-1} \circ \sigma$.
If say $\sigma'^{-1} \circ \sigma$ sends $\sqrt{A}$ to $-\sqrt{A}$ and $\sqrt{AB}$ to $-\sqrt{AB}$ then it sends $s = a + b\sqrt{A} + c\sqrt{B} + d\sqrt{AB}$ to $s = a - b\sqrt{A} + c\sqrt{B} - d\sqrt{AB}$ which implies that $b, d = 0$. This means that $\mathbf{Q}(s) = \mathbf{Q}(\sqrt{B})$. A similar argument shows the same for the other options.

Let $H \subset \mathrm{Aut}(K/\mathbf{Q})$, and let $K^H = \{a \in K \mid \sigma(a) = a \text{ for each } \sigma \in H\}$. We therefore have shown that sending a subgroup of $\mathrm{Aut}(K/\mathbf{Q})$ to the field fixed by it gives a precise correspondence between subgroups of $\mathrm{Aut}(K/\mathbf{Q})$ and intermediate fields of $K/\mathbf{Q}$

$$H \subset \mathrm{Aut}(K/\mathbf{Q}) \qquad \longmapsto \qquad K^H \subset K$$





[2]It was mentioned in the lecture that K is itself fixed by the trivial group and $\mathbf{Q}$ by $\mathrm{Aut}(K/\mathbf{Q})$, which follows from the definitions. To complete the argument we need to show that any other field fixed by either the trivial group or $\mathrm{Aut}(K/\mathbf{Q})$ is respectively K or $\mathbf{Q}$. But if subfield is not quadratic, then we have already shown that it is K or $\mathbf{Q}$. The remainder of these notes show that if a field is quadratic then it is fixed by a subgroup as above.