EXAMPLES OF THE GALOIS CORRESPONDENCE

TIM SMITS

Galois proved the following theorem (at the age of 18!), providing a link between field theory and group theory (although historically, the latter was not developed until *after* Galois had proven his theorem).

Theorem 0.1 (Galois)**.** *Let K/F be a Galois extension, and let $G = Gal(K/F)$. There is a bijection between the set $\{L : F \subset L \subset K\}$ of intermediate extensions of K and the set $\{H \leq G\}$ of subgroups of G given by $L \mapsto Gal(K/L)$ and $K^H \leftarrow\!\shortmid H$. This bijection has the following properties:*

1. *(Inclusion reversing) If L_1, L_2 are intermediate fields with associated subgroups H_1, H_2 then $L_1 \subset L_2 \iff H_2 \leq H_1$.*
2. *$[K : L] = |H|$ and $[L : F] = [G : H]$.*
3. *For two subfields L, L' we have $L \cong L' \iff H, H'$ are conjugate subgroups in G. In particular, $Gal(K/\sigma(L)) = \sigma Gal(K/L)\sigma^{-1}$ for $\sigma \in Gal(K/F)$.*
4. *L/F is Galois $\iff H \trianglelefteq G$, in which case the restriction map $\sigma \mapsto \sigma|_L$ from $Gal(K/F) \to Gal(L/F)$ is surjective with kernel $Gal(K/L)$, and so gives an isomorphism $G/H \cong Gal(L/F)$.*

Note that since K/F is Galois (and therefore separable), L/F is separable so in property (4) saying L/F is Galois is equivalent to saying that L/F is *normal* (hence, the terminology!). The subgroup structure of the Galois group gives us immediate information about the number/degrees of intermediate extensions, but that doesn't necessarily mean that finding all intermediate extensions is an easy task. Our goal is to explicitly work out examples of the correspondence.

Example 0.2. Consider $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, which is the splitting field of $(x^2 - 2)(x^2 - 3)$, so it's Galois. The polynomial $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$ because it it has no rational root, so $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ has degree 2, and one can show that $x^2 - 3$ is irreducible in $\mathbb{Q}(\sqrt{2})[x]$ by checking that there is no element of $\mathbb{Q}(\sqrt{2})$ that squares to 3. Therefore, $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is a degree 4 extension, so the Galois group has order 4. Any automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ is determined by it's action on the generators $\sqrt{2}$ and $\sqrt{3}$. Since σ must map elements to roots of their minimal polynomials, we see that $\sigma(\sqrt{2}) \in \{\pm\sqrt{2}\}$ and $\sigma(\sqrt{3}) \in \{\pm\sqrt{3}\}$, so there are at most $2 \cdot 2 = 4$ possible automorphisms. Since there are exactly 4, **all of these choices must work**.

Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ be the automorphism defined by $\sqrt{2} \mapsto -\sqrt{2}$ and $\sqrt{3} \mapsto \sqrt{3}$, and $\tau \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ be the automorphism defined by $\sqrt{2} \mapsto \sqrt{2}$ and $\sqrt{3} \mapsto \sqrt{3}$. Then one can check that $\{1, \sigma, \tau, \sigma\tau\}$ is a set of four distinct automorphisms, so it must be all of them. This tells us that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The four automorphisms and their values on the generators are listed in the table below. We'll need to know later what σ does to $\sqrt{6}$, so it's listed for convenience.

	1	σ	τ	$\sigma\tau$
$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$
$\sqrt{6}$	$\sqrt{6}$	$-\sqrt{6}$	$-\sqrt{6}$	$\sqrt{6}$

The lattice of subgroups of $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ (identified with $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$) is as follows:

$$\begin{tikzcd}
 & 1 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle\sigma\rangle \arrow[dr, dash] & \langle\sigma\tau\rangle \arrow[d, dash] & \langle\tau\rangle \arrow[dl, dash] \\
 & \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} &
\end{tikzcd}$$

which corresponds to the diagram of intermediate extensions

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
? \arrow[dr, dash] & ? \arrow[d, dash] & ? \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

with three degree 2 extensions.

Let's figure out what they are. To do so, we need to compute the fixed fields of the three different subgroups. Any element $\alpha\in\mathbb{Q}(\sqrt{2},\sqrt{3})$ looks like $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ for some $a,b,c,d\in\mathbb{Q}$. Suppose that α is fixed by σ. Since σ fixes $\mathbb{Q}$, we have $\sigma(\alpha)=a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$ using the values from the table. In particular, saying $\alpha=\sigma(\alpha)$ means that $2b\sqrt{2}+2d\sqrt{6}=0$, so that $b=d=0$ because $\sqrt{2},\sqrt{6}$ are linearly independent over $\mathbb{Q}$, being part of a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$. This says that $\mathbb{Q}(\sqrt{2},\sqrt{3})^{\langle\sigma\rangle}=\{a+c\sqrt{3}: a,c\in\mathbb{Q}\}=\mathbb{Q}(\sqrt{3})$. A similar computation shows that $\mathbb{Q}(\sqrt{2},\sqrt{3})^{\langle\tau\rangle}=\mathbb{Q}(\sqrt{2})$ and

$\mathbb{Q}(\sqrt{2}, \sqrt{3})^{\langle \sigma\tau \rangle} = \mathbb{Q}(\sqrt{6})$. Therefore, the complete diagram of intermediate extensions is given below:

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{3}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash] & \mathbb{Q}(\sqrt{2}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Example 0.3. Let $f(x) = x^3 - 2$. Then $f(x)$ is irreducible because it's Eisenstein at 2. The roots of $f(x)$ are $\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}$ where ζ_3 is a primitive cube root of unity, and so we see that the splitting field of $f(x)$ is given by $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ has degree 3 because $f(x)$ is irreducible, and note that $\zeta_3 \notin \mathbb{Q}(\sqrt[3]{2})$ because this is a subfield of $\mathbb{R}$. Since ζ_3 is a root of $x^2 + x + 1$, this tells us that $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ has degree 6. Therefore, the Galois group is a group of order 6. What group is it? Any automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q})$ is determined by it's action on the generators $\sqrt[3]{2}$ and ζ_3. Since these must be mapped to roots of their respective minimal polynomials, we see $\sigma(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}\}$ and $\sigma(\zeta_3) \in \{\zeta_3, \zeta_3^2\}$. This says there are at most $3 \cdot 2 = 6$ possible choices for an automorphism, and because we have exactly 6 automorphisms, **all of these choices must work**.

Let σ be the automorphism defined by $\sqrt[3]{2} \mapsto \zeta_3\sqrt[3]{2}$ and $\zeta_3 \mapsto \zeta_3$, and let τ be the automorphism defined by $\sqrt[3]{2} \mapsto \sqrt[3]{2}$ and $\zeta_3 \mapsto \zeta_3^2$. Then one can check that $\sigma\tau \neq \tau\sigma$, so $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) \cong S_3$ must be the non-abelian group of order 6. The six automorphisms and their values on the generators are listed in the table below.

	1	σ	σ^2	τ	$\tau\sigma$	$\tau\sigma^2$
$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\zeta_3\sqrt[3]{2}$	$\zeta_3^2\sqrt[3]{2}$	$\sqrt[3]{2}$	$\zeta_3^2\sqrt[3]{2}$	$\zeta_3\sqrt[3]{2}$
ζ_3	ζ_3	ζ_3	ζ_3	ζ_3^2	ζ_3^2	ζ_3^2

To make our isomorphism explicit, we can do the following. Label the three roots $\zeta_3^i\sqrt[3]{2}$ for $i = 0, 1, 2$ of $x^3 - 2$ as $1, 2, 3$ respectively. Then σ is identified with the permutation (123) and τ is identified with the permutation (23), so there is an explicit isomorphism between $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q})$ and S_3 given by $\sigma \mapsto (123)$ and $\tau \mapsto (23)$ (because $S_3 = \langle (123), (23) \rangle$). The lattice of subgroups of S_3 (identified with $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q})$) is given below:

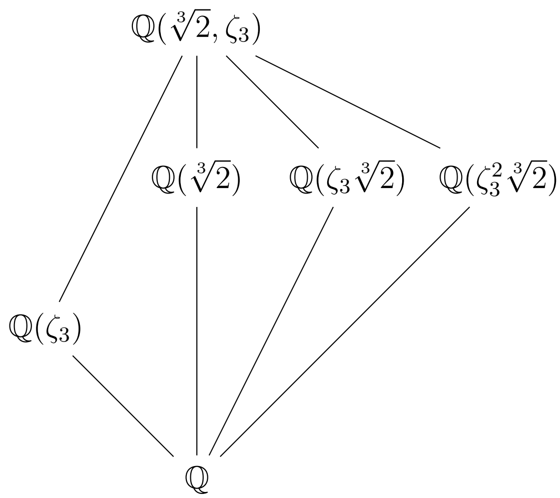
$$
\begin{tikzcd}[column sep=small]
 & 1 \arrow[dl, dash] \arrow[ddl, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
 & \langle \tau \rangle \arrow[dd, dash] & \langle \tau\sigma \rangle \arrow[ddl, dash] & \langle \tau\sigma^2 \rangle \arrow[ddll, dash] \\
\langle \sigma \rangle \arrow[dr, dash] & & & \\
 & S_3 & &
\end{tikzcd}
$$

which corresponds to the diagram of intermediate fields:

$$
\begin{tikzcd}[column sep=small]
 & \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \arrow[d, dash] \arrow[ddl, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
 & ? \arrow[dd, dash] & ? \arrow[ddl, dash] & ? \arrow[ddll, dash] \\
? \arrow[dr, dash] & & & \\
 & \mathbb{Q} & &
\end{tikzcd}
$$

with one degree 2 extension and three degree 3 extensions.

We now need to compute the fixed field of each subgroup. First, let's find the quadratic extension. This is quite easy to see by inspection: $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ obviously contains $\mathbb{Q}(\zeta_3)$ which has degree two over $\mathbb{Q}$, and therefore it must equal $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)^{\langle \sigma \rangle}$. From the table, we note that τ fixes $\sqrt[3]{2}$, and therefore this says that $\mathbb{Q}(\sqrt[2]{3}) \subset \mathbb{Q}(\sqrt[3]{2}, \zeta_3)^{\langle \tau \rangle}$. Since $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ has degree 3, they must be equal. Similarly, we see that $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)^{\langle \tau\sigma \rangle} = \mathbb{Q}(\zeta_3 \sqrt[3]{2})$ and $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)^{\langle \tau\sigma^2 \rangle} = \mathbb{Q}(\zeta_3^2 \sqrt[3]{2})$ (both of these fields have degree 3 because they're constructed by adjoining a root of of the irreducible polynomial $x^3 - 2$ to $\mathbb{Q}$). This says the complete diagram of intermediate fields is given below:



Example 0.4. Let $f(x) = x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$. Then $f(x)$ is irreducible over $\mathbb{Q}$ because it's Eisenstein at 2. Writing f as a quadratic in x^2 and using the quadratic formula, one finds that the roots of f are $\pm\sqrt{1 \pm \sqrt{3}}$. Let $\alpha = \sqrt{1+\sqrt{3}}$, $\beta = \sqrt{1-\sqrt{3}}$, so the roots are $\pm\alpha, \pm\beta$. We have $\alpha\beta = i\sqrt{2}$, and so $\beta = \frac{i\sqrt{2}}{\alpha}$. We see that $f(x)$ splits in $\mathbb{Q}(\alpha, i\sqrt{2})$ and since the splitting field of f contains $\pm\alpha, \pm\beta$, in particular it contains $i\sqrt{2}$ so the splitting field *is* $\mathbb{Q}(\alpha, i\sqrt{2})$. Since $f(x)$ is irreducible, $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a degree 4 extension, and because $\mathbb{Q}(\alpha)$ is a subfield of $\mathbb{R}$, the polynomial x^2+2 is irreducible over $\mathbb{Q}(\alpha)$ because it's roots $\pm i\sqrt{2}$ are not real. Therefore, $\mathbb{Q}(\alpha, i\sqrt{2})/\mathbb{Q}$ has degree 8. What is it's Galois group? The Galois group is a group of order 8 because the extension has degree 8. For any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\alpha, i\sqrt{2})/\mathbb{Q})$, σ is completely determined by it's action on the generators α and $i\sqrt{2}$. Since σ fixes $\mathbb{Q}$, σ must map $\alpha, i\sqrt{2}$ to a root of their respective minimal polynomials. Therefore, $\sigma(\alpha) \in \{\pm\alpha, \pm\beta\}$ and $\sigma(i\sqrt{2}) \in \{\pm i\sqrt{2}\}$. This says there are at most $4 \cdot 2 = 8$ possible different choices of automorphisms, and since we know there are exactly 8 automorphisms, **all of these choices must work**.

We now need to narrow down what the Galois group is. There are five groups of order 8: $\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, D_8, and Q_8. Let σ denote the automorphism that sends $\alpha \mapsto \beta$ and $i\sqrt{2} \mapsto -i\sqrt{2}$, and let τ denote the automorphism that sends $\alpha \mapsto \alpha$ and $i\sqrt{2} \mapsto -i\sqrt{2}$. First, one can check that $\sigma\tau \neq \tau\sigma$, because $(\sigma\tau)(\alpha) = \beta$ while $(\tau\sigma)(\alpha) = -\beta$. Therefore, it's either D_8 or Q_8. Next, note that σ^2 and $\tau\sigma$ are two distinct elements of order 2, so our Galois group is D_8. We can write down all the elements of the Galois group by filling out the table below. It will be needed later to know what the automorphisms do to β, so we will also add in this row now for convenience.

	1	σ	σ^2	σ^3	τ	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$
α	α	β	$-\alpha$	$-\beta$	α	$-\beta$	$-\alpha$	β
$i\sqrt{2}$	$i\sqrt{2}$	$-i\sqrt{2}$	$i\sqrt{2}$	$-i\sqrt{2}$	$-i\sqrt{2}$	$i\sqrt{2}$	$-i\sqrt{2}$	$i\sqrt{2}$
β	β	$-\alpha$	$-\beta$	α	$-\beta$	$-\alpha$	β	α

For the sake of making our isomorphism explicit, check that $\sigma^4 = \tau^2 = 1$ and $\tau\sigma\tau = \sigma^3$, so that there's a group isomorphism $D_8 \cong \mathrm{Gal}(\mathbb{Q}(\alpha, i\sqrt{2})/\mathbb{Q})$ given by $r \mapsto \sigma$ and $s \mapsto \tau$, recalling that $D_8 = \langle r, s | r^4 = s^2 = 1, srs = r^3 \rangle$. The lattice of subgroups of $\mathrm{Gal}(\mathbb{Q}(\alpha, i\sqrt{2})/\mathbb{Q})$ is given below:

$$\begin{tikzcd}[arrows=dash]
 & & 1 \arrow[dll] \arrow[dl] \arrow[d] \arrow[dr] \arrow[drr] & & \\
\langle \tau \rangle \arrow[dr] & \langle \tau\sigma^2 \rangle \arrow[d] & \langle \sigma^2 \rangle \arrow[dl] \arrow[d] \arrow[dr] & \langle \tau\sigma \rangle \arrow[d] & \langle \tau\sigma^3 \rangle \arrow[dl] \\
 & \langle \tau, \tau\sigma^2 \rangle \arrow[dr] & \langle \sigma \rangle \arrow[d] & \langle \tau\sigma, \tau\sigma^3 \rangle \arrow[dl] & \\
 & & D_8 & &
\end{tikzcd}$$

and so this corresponds to the diagram of intermediate fields:

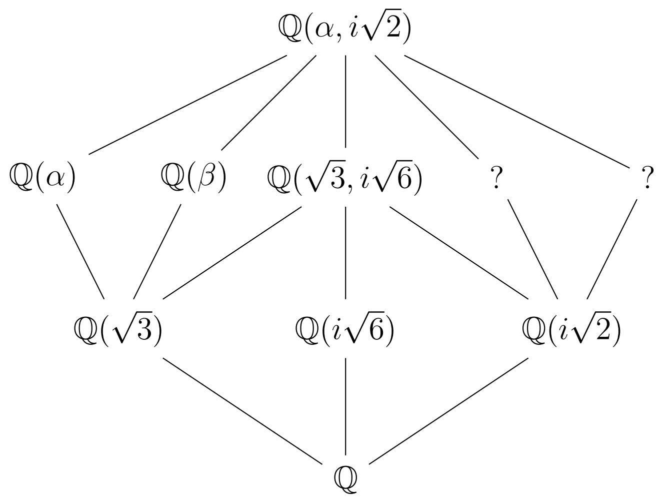
$$\begin{tikzcd}[arrows=dash]
 & & \mathbb{Q}(\alpha, i\sqrt{2}) \arrow[dll] \arrow[dl] \arrow[d] \arrow[dr] \arrow[drr] & & \\
? \arrow[dr] & ? \arrow[d] & ? \arrow[dl] \arrow[d] \arrow[dr] & ? \arrow[d] & ? \arrow[dl] \\
 & ? \arrow[dr] & ? \arrow[d] & ? \arrow[dl] & \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

with three degree 2 extensions and five degree 4 extensions.

In order to find the intermediate fields, we need to compute the fixed fields of each subgroup of $\mathrm{Gal}(\mathbb{Q}(\alpha, i\sqrt{2})/\mathbb{Q})$. There are a few subfields we can quite easily fill in by inspection. Let's start with the quadratic ones. Firstly, $\mathbb{Q}(i\sqrt{2})$ must be on our list. Also observe that since $\alpha = \sqrt{1+\sqrt{3}}$, that $\alpha^2 - 1 = \sqrt{3}$, so $\mathbb{Q}(\sqrt{3})$ is on our list. Finally, note that $i\sqrt{2} \cdot \sqrt{3} = i\sqrt{6}$ and so $\mathbb{Q}(i\sqrt{6})$ must be on our list. We've written down three quadratic extensions, and I claim they're actually all distinct, so they must be the only quadratic extensions. To do so, we just need to show that each subfield is fixed by distinct subgroups of $\mathrm{Gal}(\mathbb{Q}(\alpha, i\sqrt{2})/\mathbb{Q})$, so that they're distinct fields via the correspondence. From the table, we see that $i\sqrt{2}$ is fixed by $\tau\sigma$ and $\tau\sigma^3$, so $\mathbb{Q}(i\sqrt{2}) \subset \mathbb{Q}(\alpha, i\sqrt{2})^{\langle \tau\sigma, \tau\sigma^3 \rangle}$. Since both extensions are quadratic, they must therefore be equal. To compute the action of an element of the Galois group on $\sqrt{3}$ and $i\sqrt{6}$, we must write these in terms of α and $i\sqrt{2}$. We have $\sqrt{3} = \alpha^2 - 1$ and $i\sqrt{6} = (\alpha^2-1)i\sqrt{2}$, and so we can use the corresponding values in the table to see what happens. Doing so, one sees that $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\alpha, i\sqrt{2})^{\langle \tau, \tau\sigma^2\rangle}$ and $\mathbb{Q}(i\sqrt{6}) = \mathbb{Q}(\alpha, i\sqrt{2})^{\langle \sigma \rangle}$. Therefore, we've found all the quadratic extensions.

We can also find some quartic extensions by inspection. We saw earlier that $\mathbb{Q}(\alpha)$ is one such extension. For the same reason, $\mathbb{Q}(\beta)/\mathbb{Q}$ also has degree 4, and $\mathbb{Q}(\alpha) \neq \mathbb{Q}(\beta)$ because β is not real while α is. To get another extension, we just take a compositum of two quadratic extensions: $\mathbb{Q}(\sqrt{3}, i\sqrt{2})/\mathbb{Q}$ has degree 4. Now once more, we can show that this is distinct from the other two fields by just checking that each field is fixed by a different subgroup of the Galois group. Using the table, $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha, i\sqrt{2})^{\langle \tau \rangle}$ and so they're equal because they have the same degree. Similarly, $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha, i\sqrt{2})^{\langle \tau\sigma^2 \rangle}$, and $\mathbb{Q}(\sqrt{3}, i\sqrt{6}) = \mathbb{Q}(\alpha, i\sqrt{2})^{\langle \sigma^2 \rangle}$.

So far, we've filled out this much of the diagram:



There are two more missing quartic extensions on our list that we need to find, corresponding to the fixed fields of $\langle \tau\sigma \rangle$ and $\langle \tau\sigma^3 \rangle$ respectively. It now appears as if we've hit a wall: if you write down an arbitrary element of $\mathbb{Q}(\alpha, i\sqrt{2})$, it looks like $c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 + c_4 i\sqrt{2} + c_5\alpha i\sqrt{2} + c_6\alpha^2 i\sqrt{2} + c_7\alpha^3 i\sqrt{2}$ for $c_i \in \mathbb{Q}$. Unfortunately, $\tau\sigma$ and $\tau\sigma^3$ map α to $\pm\beta$ and we don't have an expression for β in terms of this basis. One *could* go write it down, but it's not very nice. Instead, we'll do the following.

We know that $\mathbb{Q}(\alpha, i\sqrt{2})$ is the splitting field of $x^4 - 2x^2 - 2$, so in particular, $\mathbb{Q}(\alpha, i\sqrt{2}) = \mathbb{Q}(\pm\alpha, \pm\beta)$. An element of $\mathrm{Gal}(\mathbb{Q}(\alpha, i\sqrt{2})/\mathbb{Q})$ is then *also* determined by it's actions on $\pm\alpha, \pm\beta$, which must map to one of the four roots of $x^4 - 2x^2 - 2$. If we label the four roots $\alpha, -\alpha, \beta, -\beta$ as $1, 2, 3, 4$ respectively, we may view $\mathrm{Gal}(\mathbb{Q}(\alpha, i\sqrt{2})/\mathbb{Q})$ as a subgroup of S_4 by writing our different automorphisms as permutations. We see from the table that $\tau\sigma = (14)(23)$ and $\tau\sigma^3 = (13)(24)$ as permutations. In other words, $\tau\sigma$ swaps roots $1, 4$ and $2, 3$. Therefore, the element $\alpha - \beta$, corresponding to the sum of roots 1 and 4, is *fixed* by $\tau\sigma$! This says $\mathbb{Q}(\alpha - \beta) \subset \mathbb{Q}(\alpha, i\sqrt{2})^{\langle \tau\sigma \rangle}$. Similarly, $\mathbb{Q}(\alpha + \beta) \subset \mathbb{Q}(\alpha, i\sqrt{2})^{\langle \tau\sigma^3 \rangle}$. To show equality, we need to compute the degrees of these extensions. To do so, we need to compute the orbits of $\alpha - \beta$ and $\alpha + \beta$ under the action of the Galois group. Using our table one last time, the different values that we obtain by hitting each of $\alpha - \beta$ and $\alpha + \beta$ by the various elements of the Galois group are $\pm\alpha \pm \beta$, so that their minimal polynomial has degree 4. This says the extensions have degree 4, so we're done! The complete diagram of intermediate extensions is then as follows:

$$
\begin{tikzcd}
 & & \mathbb{Q}(\alpha, i\sqrt{2}) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\alpha) \arrow[dr, dash] & \mathbb{Q}(\beta) \arrow[d, dash] & \mathbb{Q}(\sqrt{3}, i\sqrt{6}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}(\alpha-\beta) \arrow[d, dash] & \mathbb{Q}(\alpha+\beta) \arrow[dl, dash] \\
 & \mathbb{Q}(\sqrt{3}) \arrow[dr, dash] & \mathbb{Q}(i\sqrt{6}) \arrow[d, dash] & \mathbb{Q}(i\sqrt{2}) \arrow[dl, dash] & \\
 & & \mathbb{Q} & &
\end{tikzcd}
$$

Remark 0.5. One might wonder why we didn't write our extension as $\mathbb{Q}(\alpha, \beta)$ to begin with, if in the end this is what we needed to find the last two extensions. The reason is simply because we wouldn't be able to immediately get the correct bound for the size of the Galois group: α, β must map to roots of $x^4 - 2x^2 - 2$ (and they can't map to the same thing), so there would be at most $4 \cdot 3 = 12$ choices for σ. Obviously this doesn't help, because we know there are exactly 8, so some of the choices won't work! To cut down the bound, note that $\alpha + \beta \neq 0$, and therefore $\sigma(\beta) \neq -\sigma(\alpha)$. Since we already require $\sigma(\beta) \neq \sigma(\alpha)$, this gives at most $4 \cdot 2 = 8$ automorphisms, and therefore we can write them down. Working with the basis $\{1, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta\}$ of $\mathbb{Q}(\alpha, \beta)/\mathbb{Q}$, you can then explicitly determine what the fixed fields are by computing the Galois action of each of the 8 automorphisms in the table on an arbitrary element of $\mathbb{Q}(\alpha, \beta)$, and seeing what conditions on the coefficients have to hold for it to be fixed. You can check yourself as an exercise that you'll get the following diagram, now with all the generators expressed in terms of α and β.

$$
\begin{tikzcd}
 & & \mathbb{Q}(\alpha, \beta) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\alpha) \arrow[dr, dash] & \mathbb{Q}(\beta) \arrow[d, dash] & \mathbb{Q}(\alpha^2, \alpha\beta) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \mathbb{Q}(\alpha-\beta) \arrow[d, dash] & \mathbb{Q}(\alpha+\beta) \arrow[dl, dash] \\
 & \mathbb{Q}(\alpha^2) \arrow[dr, dash] & \mathbb{Q}(\alpha^3\beta - \alpha\beta) \arrow[d, dash] & \mathbb{Q}(\alpha\beta) \arrow[dl, dash] & \\
 & & \mathbb{Q} & &
\end{tikzcd}
$$