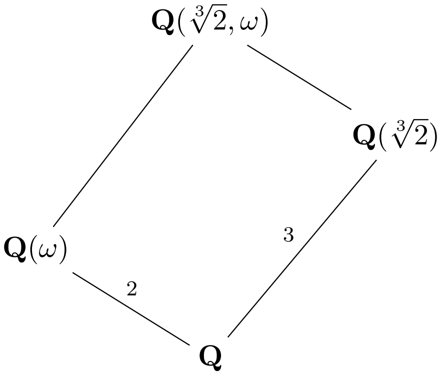
SOME EXAMPLES OF THE GALOIS CORRESPONDENCE

KEITH CONRAD

Example 1. The field extension $\mathbf{Q}(\sqrt[3]{2},\omega)/\mathbf{Q}$, where ω is a nontrivial cube root of unity, is Galois: it is a splitting field over $\mathbf{Q}$ for X^3-2, which is separable since every irreducible in $\mathbf{Q}[X]$ is separable. The number of field automorphisms of $\mathbf{Q}(\sqrt[3]{2},\omega)/\mathbf{Q}$ is $[\mathbf{Q}(\sqrt[3]{2},\omega):\mathbf{Q}]=6$. (For comparison, the number of field automorphisms of $\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}$ is 1, even though the field extension has degree 3: there is just nowhere for $\sqrt[3]{2}$ to go in $\mathbf{Q}(\sqrt[3]{2})$ except to itself.) We will give *two* ways to think about $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2},\omega)/\mathbf{Q})$.



For the first way, each σ in $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2},\omega)/\mathbf{Q})$ is determined by its effect on the 3 roots of X^3-2, which are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$: these roots generate the top field over the bottom field (note $\omega=\omega\sqrt[3]{2}/\sqrt[3]{2}$ is a ratio of two cube roots of 2). There are at most 6 permutations of these 3 roots, and since we know there are 6 automorphisms, each permutation of the roots comes from an automorphism of the field extension. Thus $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2},\omega)/\mathbf{Q})\cong S_3$ with S_3 thought of as the symmetric group on the set of 3 roots of X^3-2.

For another viewpoint, any σ in the Galois group is determined by the two values $\sigma(\sqrt[3]{2})\in\{\sqrt[3]{2},\omega\sqrt[3]{2},\omega^2\sqrt[3]{2}\}$ and $\sigma(\omega)\in\{\omega,\omega^2\}$. Therefore there are at most $3\cdot 2=6$ possibilities for σ. Since 6 is the number of automorphisms, all of these possibilities really work: each choice of a root of X^3-2 for $\sigma(\sqrt[3]{2})$ and a nontrivial cube root of unity for $\sigma(\omega)$ does come from an automorphism σ. Write $\sigma(\omega)=\omega^{a_\sigma}$ where $a_\sigma\in(\mathbf{Z}/(3))^\times$ and $\sigma(\sqrt[3]{2})=\omega^{b_\sigma}\sqrt[3]{2}$ where $b_\sigma\in\mathbf{Z}/(3)$. For two automorphisms σ and τ,

$$\sigma(\tau(\omega))=\sigma(\omega^{a_\tau})=\sigma(\omega)^{a_\tau}=\omega^{a_\sigma a_\tau}$$

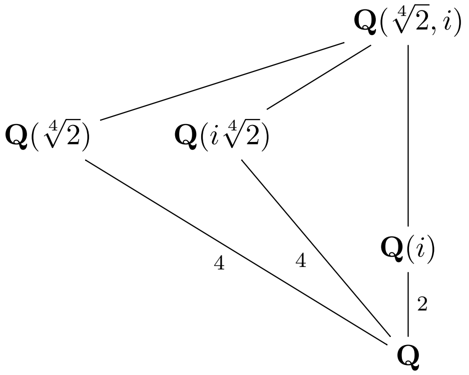
and

$$\sigma(\tau(\sqrt[3]{2}))=\sigma(\omega^{b_\tau}\sqrt[3]{2})=\sigma(\omega)^{b_\tau}\sigma(\sqrt[3]{2})=\omega^{a_\sigma b_\tau}\omega^{b_\sigma}\sqrt[3]{2}=\omega^{a_\sigma b_\tau+b_\sigma}\sqrt[3]{2}.$$

Looking at the exponents of ω on the right side of these two equations, composition of σ and τ behaves like multiplication of matrices $\left(\begin{smallmatrix} a & b\\ 0 & 1\end{smallmatrix}\right)$ with entries in $\mathbf{Z}/(3)$, since $\left(\begin{smallmatrix} a & b\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix} a' & b'\\ 0 & 1\end{smallmatrix}\right)=\left(\begin{smallmatrix} aa' & ab'+b\\ 0 & 1\end{smallmatrix}\right)$: $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2},\omega)/\mathbf{Q})$ is isomorphic to the group of mod 3 invertible matrices $\left(\begin{smallmatrix} a & b\\ 0 & 1\end{smallmatrix}\right)$ by $\sigma\mapsto\left(\begin{smallmatrix} a_\sigma & b_\sigma\\ 0 & 1\end{smallmatrix}\right)$.

That we found two models for $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2},\omega)/\mathbf{Q})$, as permutations and as matrices, is no surprise: both models are nonabelian and all nonabelian groups of order 6 are isomorphic.

Example 2. The extension $\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q}$ is Galois by the same reasoning as in the previous example: the top field is the splitting field over $\mathbf{Q}$ for X^4-2, which is separable. The diagram below shows some of the intermediate fields, but these are not all the intermediate fields. For instance, $\mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\sqrt[4]{2})$, but this is not the only missing subfield.


$\mathbf{Q}(\sqrt[4]{2},i)$
$\mathbf{Q}(\sqrt[4]{2})$
$\mathbf{Q}(i\sqrt[4]{2})$
$\mathbf{Q}(i)$
4
4
2
$\mathbf{Q}$

Although each element of $\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q})$ permutes the 4 roots of X^4-2, not all 24 permutations of the roots are realized by the Galois group. (This is a contrast to $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2},\omega)/\mathbf{Q})$!) For example, $\sqrt[4]{2}$ and $-\sqrt[4]{2}$ add to 0, so under a field automorphism these two roots go to roots that are also negatives of each other. No field automorphism of $\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q}$ could send $\sqrt[4]{2}$ to $i\sqrt[4]{2}$ and $-\sqrt[4]{2}$ to $\sqrt[4]{2}$ because that doesn't respect the algebraic relation $x+y=0$ that holds for $x=\sqrt[4]{2}$ and $y=-\sqrt[4]{2}$.

To figure out what $\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q})$ is concretely, we think about an automorphism σ by what it does to $\sqrt[4]{2}$ and i, rather than what it does to all the fourth roots of 2. Since $\sigma(\sqrt[4]{2})$ has to be a root of X^4-2 (4 possible values) and $\sigma(i)$ has to be a root of X^2+1 (2 possible values), there are at most $4\cdot 2=8$ automorphisms of $\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q}$. Because $[\mathbf{Q}(\sqrt[4]{2},i):\mathbf{Q}]=8$, $\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q})$ has size 8 and therefore all assignments of $\sigma(\sqrt[4]{2})$ and $\sigma(i)$ to roots of X^4-2 and X^2+1, respectively, *must* be realized by field automorphisms. Let r and s be the automorphisms of $\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q}$ determined by

$$r(\sqrt[4]{2}) = i\sqrt[4]{2}, \quad r(i)=i, \quad s(\sqrt[4]{2})=\sqrt[4]{2}, \quad s(i)=-i.$$

By taking powers and products (that is, composites) of automorphisms, we obtain the following table of 8 different automorphisms of $\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q}$. (They are different because they don't have the same effect on both $\sqrt[4]{2}$ and i, which generate the field extension).

σ	id	r	r^2	r^3	s	rs	r^2s	r^3s
$\sigma(\sqrt[4]{2})$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$	$\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-\sqrt[4]{2}$	$-i\sqrt[4]{2}$
$\sigma(i)$	i	i	i	i	$-i$	$-i$	$-i$	$-i$

Table 1.

A calculation at $\sqrt[4]{2}$ and i shows $r^4=\mathrm{id}$, $s^2=\mathrm{id}$, and $rs=sr^{-1}$, so $\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q})$ is isomorphic (not equal, just isomorphic!) to D_4, where D_4 can be viewed as the 8 symmetries of the square whose vertices are the four complex roots of X^4-2: r is rotation by 90 degrees counterclockwise and s is complex conjugation, which is a reflection across one diagonal of this square. (Strictly speaking, r and s as automorphisms are only defined on $\mathbf{Q}(\sqrt[4]{2}, i)$, not on all complex numbers. While r looks like a rotation by 90 degrees on the four roots of $X^4 - 2$, it is not really a rotation on most elements of $\mathbf{Q}(\sqrt[4]{2})$, since r is not multiplication by i everywhere. For example, $r(1)$ is 1 rather than i, and $r(i)$ is i rather than -1. The function s, however, does coincide with complex conjugation on all of $\mathbf{Q}(\sqrt[4]{2}, i)$.)

Since $\mathbf{Q}(\sqrt[4]{2}, i)$ is a Galois extension of $\mathbf{Q}$, we can compute the degree of a number in $\mathbf{Q}(\sqrt[4]{2}, i)$ over $\mathbf{Q}$ by counting the size of its Galois orbit. For example, let

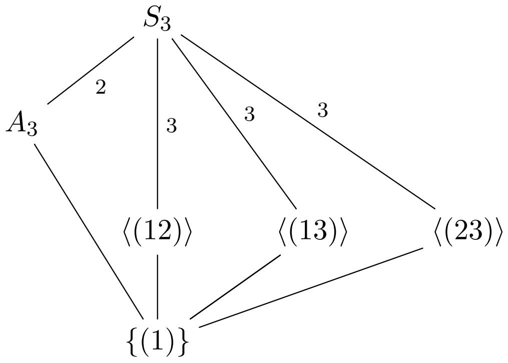
$$\alpha = \sqrt[4]{2} + \sqrt{2} + 1.$$

Applying $\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q})$ to α and seeing what different numbers come out amounts to replacing $\sqrt[4]{2}$ in the expression for α by the four different fourth roots of 2 and replacing $\sqrt{2} = \sqrt[4]{2}^2$ in the expression for α by the squares of those respective fourth roots of 2. We obtain the list

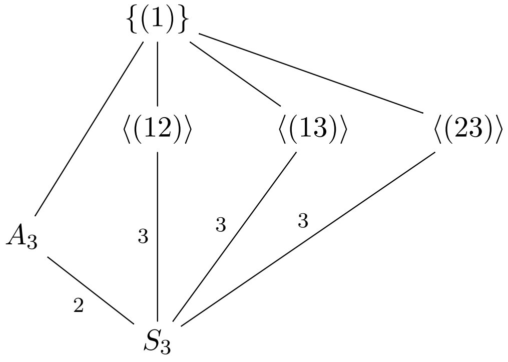
$$\sqrt[4]{2} + \sqrt{2} + 1, \quad i\sqrt[4]{2} - \sqrt{2} + 1, \quad -\sqrt[4]{2} + \sqrt{2} + 1, \quad -i\sqrt[4]{2} - \sqrt{2} + 1.$$

Although $\mathrm{Gal}(\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q})$ has size 8, the Galois orbit of α only has size 4. Therefore the field extension $\mathbf{Q}(\alpha)/\mathbf{Q}$ has degree 4. Since $\alpha \in \mathbf{Q}(\sqrt[4]{2})$, so $\mathbf{Q}(\alpha) \subset \mathbf{Q}(\sqrt[4]{2})$, a degree comparison implies $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt[4]{2})$. It is easy to see why the Galois orbit has fewer than 8 numbers in it: complex conjugation s does not change α, so every σ and σs have the same value at α.

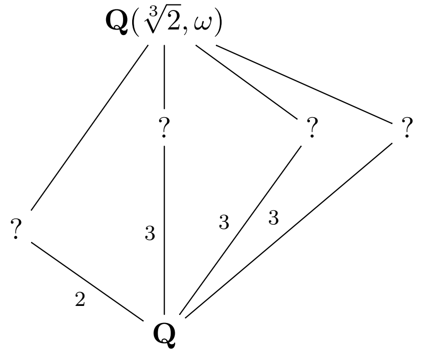
Example 3. The extension $\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q}$ has Galois group isomorphic to S_3 (Example 1). This group has 3 subgroups of order 2 and one subgroup (just A_3) of order 3. In the diagram we have indicated the indices in S_3 of subgroups.



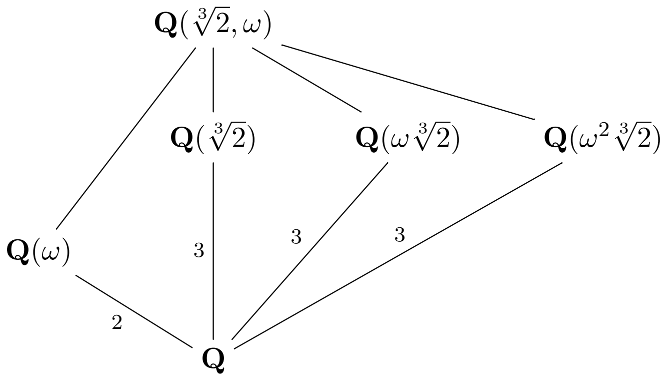
Let's flip this upside down, so larger groups are on the bottom.



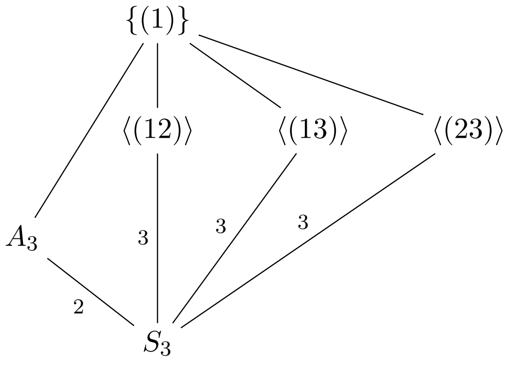
By the Galois correspondence, the arrangement of subfields of $\mathbf{Q}(\sqrt[3]{2}, \omega)$ looks the same, with indices of a subgroup in the Galois group turning into degrees of a subfield over $\mathbf{Q}$.

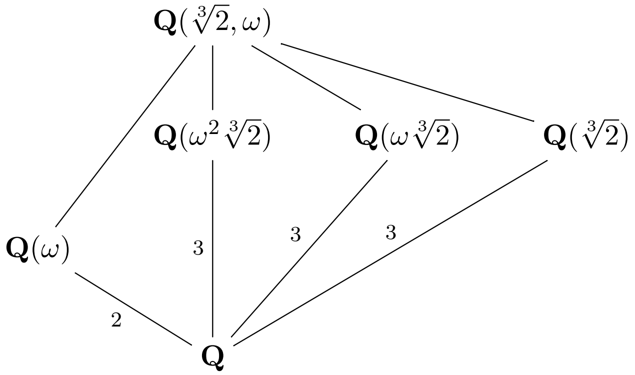


So there is one quadratic subfield and three cubic subfields. It is easy to write down enough such fields by inspection: $\mathbf{Q}(\omega)$ is quadratic and $\mathbf{Q}(\sqrt[3]{2})$, $\mathbf{Q}(\omega\sqrt[3]{2})$, and $\mathbf{Q}(\omega^2\sqrt[3]{2})$ are all cubic. (These three cubic fields are distinct since two different cube roots of 2 can't lie in the same cubic field.) So these are the only (proper) intermediate fields, and the field diagram looks like this:


$\mathbf{Q}(\sqrt[3]{2}, \omega)$
$\mathbf{Q}(\sqrt[3]{2})$
$\mathbf{Q}(\omega\sqrt[3]{2})$
$\mathbf{Q}(\omega^2\sqrt[3]{2})$
$\mathbf{Q}(\omega)$
3
3
3
2
$\mathbf{Q}$

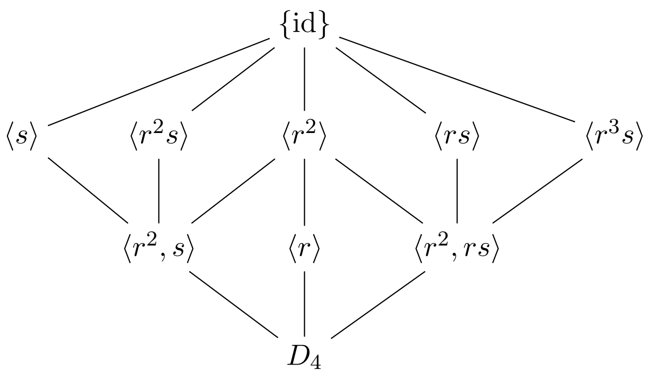
We were somewhat cavalier about the way we just wrote down the cubic fields without really paying attention to which ones should correspond to which subgroups of index 3 (order 2) in the Galois group. But we can't be more careful at this stage (beyond keeping track of indices of subgroups and degrees of subfields) because we didn't really keep track here of *how* $\mathrm{Gal}(\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q})$ is isomorphic to S_3. We simply used the subgroup structure of S_3 to figure out the subfield structure of $\mathbf{Q}(\sqrt[3]{2}, \omega)$. If we want to match specific subgroups with specific subfields through the Galois correspondence, we have to think about S_3 as the Galois group in a definite way. There are three roots of $X^3 - 2$ being permuted by the Galois group (in all 6 possible ways), so if we label these roots abstractly as 1, 2, and 3 then we can see what the correspondence should be. Label $\sqrt[3]{2}$ as 1, $\omega\sqrt[3]{2}$ as 2, and $\omega^2\sqrt[3]{2}$ as 3. Then (12) fixes $\omega^2\sqrt[3]{2}$, and therefore $\mathbf{Q}(\omega^2\sqrt[3]{2})$ is contained in the fixed field $\mathbf{Q}(\sqrt[3]{2}, \omega)^{\langle(12)\rangle}$. The subgroup $\langle(12)\rangle$ has index 3 and $\mathbf{Q}(\omega^2\sqrt[3]{2})/\mathbf{Q}$ has degree 3, so $\mathbf{Q}(\omega^2\sqrt[3]{2})$ is the full fixed field of $\langle(12)\rangle$. In a similar way, $\langle(13)\rangle$ has fixed field $\mathbf{Q}(\omega\sqrt[3]{2})$ and $\langle(23)\rangle$ has fixed field $\mathbf{Q}(\sqrt[3]{2})$. So the subgroup and subfield diagrams are aligned if we draw them as follows:



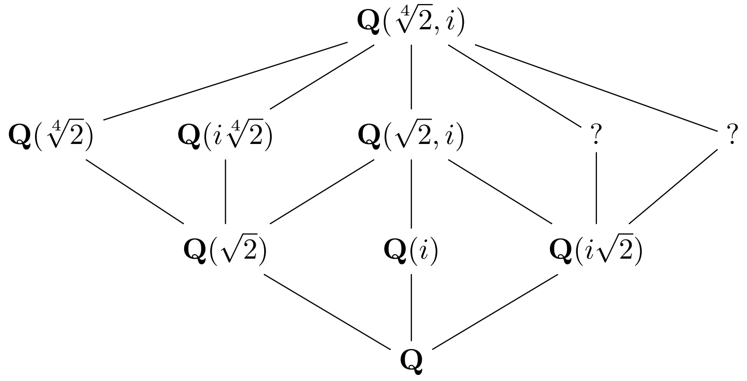

$\mathbf{Q}(\sqrt[3]{2},\omega)$
$\mathbf{Q}(\omega^2\sqrt[3]{2})$
$\mathbf{Q}(\omega\sqrt[3]{2})$
$\mathbf{Q}(\sqrt[3]{2})$
$\mathbf{Q}(\omega)$
3
3
3
2
$\mathbf{Q}$

Example 4. The extension $\mathbf{Q}(\sqrt[4]{2},i)/\mathbf{Q}$ has Galois group isomorphic to D_4 according to the permutations that the Galois group induces on the fourth roots of 2. Generators are r and s where $r(\sqrt[4]{2}) = i\sqrt[4]{2}$, $r(i) = i$ and $s(\sqrt[4]{2}) = \sqrt[4]{2}$, $s(i) = -i$ (s is complex conjugation). See Table 1 in Example 2.

Below is the diagram of all subgroups of D_4, written upside down.



All indices of successive subgroups here are 2, so we don't include that information in the diagram. The lattice of intermediate fields in $\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q}$ looks the same:


$\mathbf{Q}(\sqrt[4]{2}, i)$
$\mathbf{Q}(\sqrt[4]{2})$
$\mathbf{Q}(i\sqrt[4]{2})$
$\mathbf{Q}(\sqrt{2}, i)$
?
?
$\mathbf{Q}(\sqrt{2})$
$\mathbf{Q}(i)$
$\mathbf{Q}(i\sqrt{2})$
$\mathbf{Q}$

To check the fields have been placed correctly according to the Galois correspondence $H \rightsquigarrow \mathbf{Q}(\sqrt[4]{2}, i)^H$, verify in each case that each field in the field diagram is fixed by the subgroup in the same relative position in the subgroup diagram, and the degree of the field over $\mathbf{Q}$ equals the index of the subgroup over $\mathbf{Q}$: if $F \subset \mathbf{Q}(\sqrt[4]{2}, i)^H$ and $[F : \mathbf{Q}] = [D_4 : H]$ then $F = \mathbf{Q}(\sqrt[4]{2}, i)^H$.

For example, since $[\mathbf{Q}(i) : \mathbf{Q}] = 2$, the subgroup H in D_4 corresponding to $\mathbf{Q}(i)$ has index 2. Since $r(i) = i$, $\langle r \rangle$ is a subgroup fixing i with index $8/4 = 2$, so $H = \langle r \rangle$. Thus $\mathbf{Q}(i)$ corresponds to $\langle r \rangle$.

Two fields in the field diagram above have been left undetermined. What are they? They correspond to the subgroups $\langle rs \rangle$ and $\langle r^3 s \rangle$, which are the only nontrivial proper subgroups of $\langle r^2, rs \rangle$, so we can figure out the undetermined fields by finding an $\alpha \in \mathbf{Q}(\sqrt[4]{2}, i)$ of degree 4 over $\mathbf{Q}$ that is fixed by rs and not by r^2, and likewise finding a β of degree 4 over $\mathbf{Q}$ that is fixed by $r^3 s$ and not by r^2. Then the two missing fields are $\mathbf{Q}(\alpha)$ and $\mathbf{Q}(\beta)$.

To find α, rather than blind guessing we simply write a general α in $\mathbf{Q}(\sqrt[4]{2}, i)$ using a basis over $\mathbf{Q}$ and see what the condition $rs(\alpha) = \alpha$ says about its coefficients. Writing

$$\alpha = a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{2}^3 + ei + fi\sqrt[4]{2} + gi\sqrt{2} + hi\sqrt[4]{2}^3,$$

with rational coefficients a, b, c, d, e, f, g, h, applying rs to all terms gives

$$rs(\alpha) = a + bi\sqrt[4]{2} - c\sqrt{2} - di\sqrt[4]{2}^3 - ei + f\sqrt[4]{2} + gi\sqrt{2} - h\sqrt[4]{2}^3,$$

so the condition $rs(\alpha) = \alpha$ is equivalent to

$$b = f, \ c = -c, \ e = -e, \ d = -h.$$

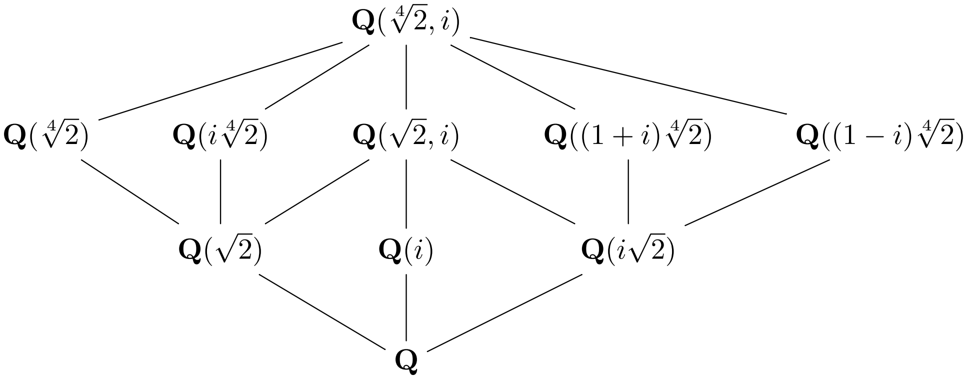
Therefore

$$\alpha = a + b(1+i)\sqrt[4]{2} + d(1-i)\sqrt[4]{2}^3 + gi\sqrt{2}.$$

The coefficients a, b, d, g can be arbitrary rational numbers. To pick something simple of degree 4, we try $b = 1$ and set the other coefficients equal to 0:

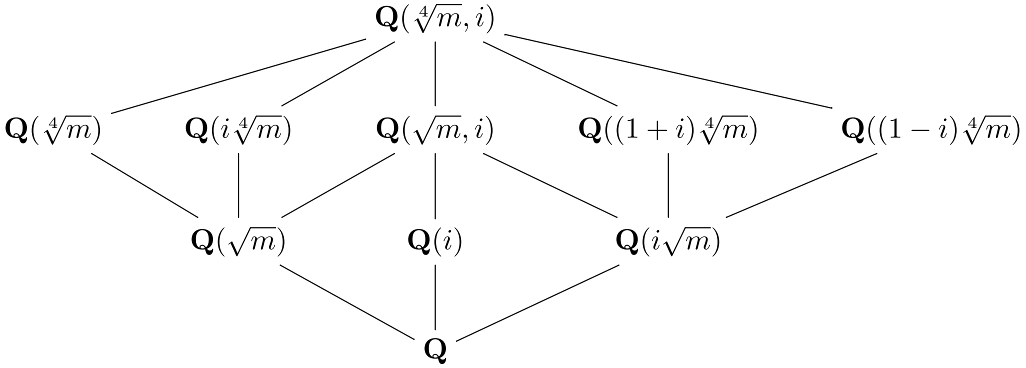
$$\alpha := (1+i)\sqrt[4]{2}.$$

With this choice of α we have $r^2(\alpha) = -\alpha$, so α is fixed by $\langle rs \rangle$ but not by $\langle r^2 \rangle$, which means the field $\mathbf{Q}(\alpha)$ is inside the fixed field of $\langle rs \rangle$ but is not inside the fixed field of $\langle r^2 \rangle$, so $\mathbf{Q}(\alpha)$ must be the fixed field of $\langle rs \rangle$. The number $\beta = (1-i)\sqrt[4]{2}$ is fixed by $r^3 s$ and not by r^2, so the fixed field of $\langle r^3 s\rangle$ is $\mathbf{Q}((1-i)\sqrt[4]{2})$. Now we have a complete field diagram corresponding to the subgroup diagram of D_4 at the start of this example.


$\mathbf{Q}(\sqrt[4]{2}, i)$
$\mathbf{Q}(\sqrt[4]{2})$
$\mathbf{Q}(i\sqrt[4]{2})$
$\mathbf{Q}(\sqrt{2}, i)$
$\mathbf{Q}((1+i)\sqrt[4]{2})$
$\mathbf{Q}((1-i)\sqrt[4]{2})$
$\mathbf{Q}(\sqrt{2})$
$\mathbf{Q}(i)$
$\mathbf{Q}(i\sqrt{2})$
$\mathbf{Q}$

Note $(1+i)\sqrt[4]{2}$ and $(1-i)\sqrt[4]{2}$ are both roots of X^4+8, so the distinct but isomorphic fields $\mathbf{Q}((1+i)\sqrt[4]{2})$ and $\mathbf{Q}((1-i)\sqrt[4]{2})$ are analogous to the fields $\mathbf{Q}(\sqrt[4]{2})$ and $\mathbf{Q}(i\sqrt[4]{2})$ that are each generated by a root of X^4-2.

All of this work generalizes to the splitting field of X^4-m over $\mathbf{Q}$ for nonzero $m \in \mathbf{Z}$ if we assume X^4-m is irreducible over $\mathbf{Q}$ and $\boxed{m \neq -n^2}$ (so $\mathbf{Q}(\sqrt{m}) \neq \mathbf{Q}(i)$). Writing $\sqrt[4]{m}$ for one root of X^4-m, the splitting field of X^4-m over $\mathbf{Q}$ is $\mathbf{Q}(\sqrt[4]{m}, i)$, whose Galois group over $\mathbf{Q}$ is isomorphic to D_4 and the diagram below describes all of its subfields, with $(1 \pm i)\sqrt[4]{m}$ being roots of X^4+4m.

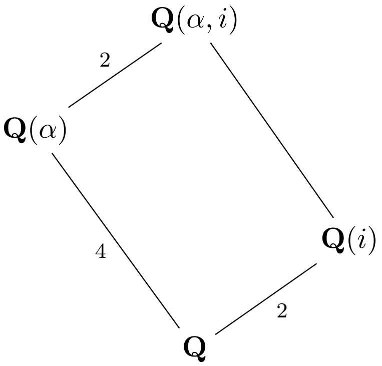

$\mathbf{Q}(\sqrt[4]{m}, i)$
$\mathbf{Q}(\sqrt[4]{m})$
$\mathbf{Q}(i\sqrt[4]{m})$
$\mathbf{Q}(\sqrt{m}, i)$
$\mathbf{Q}((1+i)\sqrt[4]{m})$
$\mathbf{Q}((1-i)\sqrt[4]{m})$
$\mathbf{Q}(\sqrt{m})$
$\mathbf{Q}(i)$
$\mathbf{Q}(i\sqrt{m})$
$\mathbf{Q}$

The restriction $m \neq -n^2$ above is important, because without it the splitting field of X^4-m over $\mathbf{Q}$ does not have degree 8. For example, taking $n=1$ and $m=-n^2=-1$, the polynomial X^4+1 is irreducible over $\mathbf{Q}$ (replacing X by $X+1$ makes it Eisenstein at 2) and its splitting field over $\mathbf{Q}$ is $\mathbf{Q}(\zeta_8)$ since X^4+1 is the 8th cyclotomic polynomial, with $\mathrm{Gal}(\mathbf{Q}(\zeta_8)/\mathbf{Q}) \cong (\mathbf{Z}/8\mathbf{Z})^\times$, which is of order 4 and each nontrivial element has order 2. More generally, if $m=-n^2$ then in is a square root of m, $\gamma := \sqrt{in}$ is a fourth root of m, and $i = \gamma^2/n$ is inside $\mathbf{Q}(\gamma)$. If $m=-n^2$ and X^4-m is irreducible over $\mathbf{Q}$, its splitting field over $\mathbf{Q}$ is $\mathbf{Q}(\gamma, i) = \mathbf{Q}(\gamma)$, which has degree 4 over $\mathbf{Q}$[1] and in $\mathrm{Gal}(\mathbf{Q}(\gamma)/\mathbf{Q})$ the nontrivial elements have order 2: the $\mathbf{Q}$-conjugates of γ are $\pm\gamma$ and $\pm i\gamma$, and if $\sigma(\gamma) = -\gamma$ then $\sigma(i) = i$ (view i as γ^2/n) and $\sigma^2(\gamma) = \gamma$, while if $\tau(\gamma) = i\gamma$ or $-i\gamma$ then $\tau(i) = -i$ and $\tau^2(\gamma) = \gamma$ (check!).

[1] If $m=-n^2$ and X^4-m is *reducible* over $\mathbf{Q}$, then its splitting field over $\mathbf{Q}$ is $\mathbf{Q}(i)$, so of degree 2.

Example 5. The polynomial $X^4 - X^2 - 1$ is irreducible over $\mathbf{Q}$ since it is irreducible mod 3. Let's find its splitting field over $\mathbf{Q}$ and all of its subfields.

The roots of $X^4 - X^2 - 1$ are $\pm\sqrt{(1+\sqrt{5})/2}$ and $\pm\sqrt{(1-\sqrt{5})/2}$. Let $\alpha = \sqrt{(1+\sqrt{5})/2}$, so $\pm\sqrt{(1-\sqrt{5})/2} = \pm i/\alpha$. Therefore the splitting field of $X^4 - X^2 - 1$ over $\mathbf{Q}$ is $\mathbf{Q}(\alpha, i)$. Since α is real, $i \notin \mathbf{Q}(\alpha)$, so as the diagram below illustrates $[\mathbf{Q}(\alpha, i) : \mathbf{Q}] = 8$.



Any $\sigma \in \text{Gal}(\mathbf{Q}(\alpha, i)/\mathbf{Q})$ is determined by $\sigma(\alpha)$ and $\sigma(i)$. Since $\sigma(\alpha)$ has four possible values ($\pm\alpha$ and $\pm i/\alpha$) and $\sigma(i)$ has two possible values ($\pm i$), there are at most eight pairs $(\sigma(\alpha), \sigma(i))$ and hence at most 8 possibilities for σ. The group $\text{Gal}(\mathbf{Q}(\alpha, i)/\mathbf{Q})$ has order 8, so all 8 possible choices for $(\sigma(\alpha), \sigma(i))$ really do arise. See Table 2. The fifth column is complex conjugation on $\mathbf{Q}(\alpha, i)$.

$\sigma(\alpha)$	α	$-\alpha$	i/α	$-i/\alpha$	α	$-\alpha$	i/α	$-i/\alpha$
$\sigma(i)$	i	i	i	i	$-i$	$-i$	$-i$	$-i$

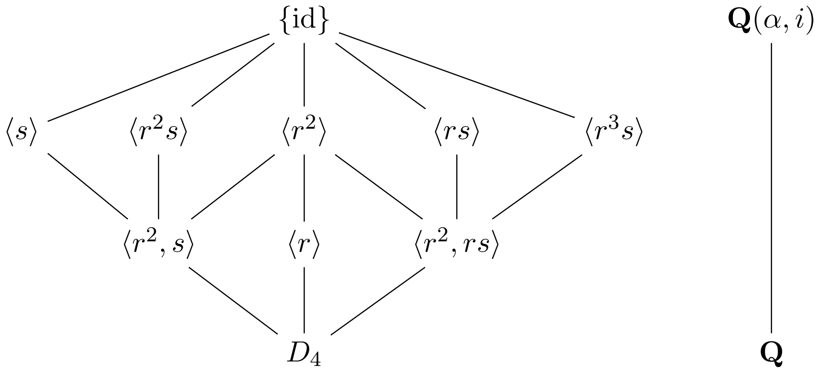
Table 2.

To help us recognize $\text{Gal}(\mathbf{Q}(\alpha, i)/\mathbf{Q})$, the last two automorphisms in Table 2 have order 4 and the other nonidentity automorphisms in the table have order 2 (check!). The extension $\mathbf{Q}(\alpha)/\mathbf{Q}$ is not Galois (after all, α has $\mathbf{Q}$-conjugate i/α, which is not in $\mathbf{Q}(\alpha)$ since i/α is not real), so $\text{Gal}(\mathbf{Q}(\alpha, i)/\mathbf{Q})$ has a non-normal subgroup and in particular is not abelian. This is enough information to pin down the Galois group up to isomorphism: the two nonabelian groups of order 8 are D_4 and Q_8, and every subgroup of Q_8 is normal, so $\text{Gal}(\mathbf{Q}(\alpha, i)/\mathbf{Q}) \cong D_4$. To make this isomorphism concrete, let r be the automorphism with the effect in the second to last column of Table 2 (it has order 4) and let s be complex conjugation on $\mathbf{Q}(\alpha, i)$. Then we can list the automorphisms described in Table 2 as in Table 3. As an exercise, check from Table 3 that $sr = r^3 s$.

σ	id	r^2	rs	r^3s	s	r^2s	r	r^3
$\sigma(\alpha)$	α	$-\alpha$	i/α	$-i/\alpha$	α	$-\alpha$	i/α	$-i/\alpha$
$\sigma(i)$	i	i	i	i	$-i$	$-i$	$-i$	$-i$

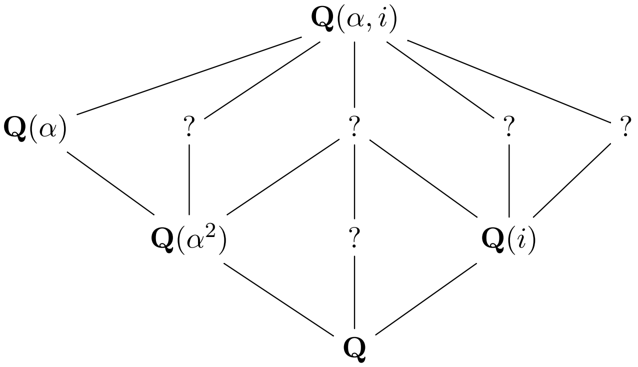
Table 3.

Below is the lattice of subgroups of D_4, upside down.

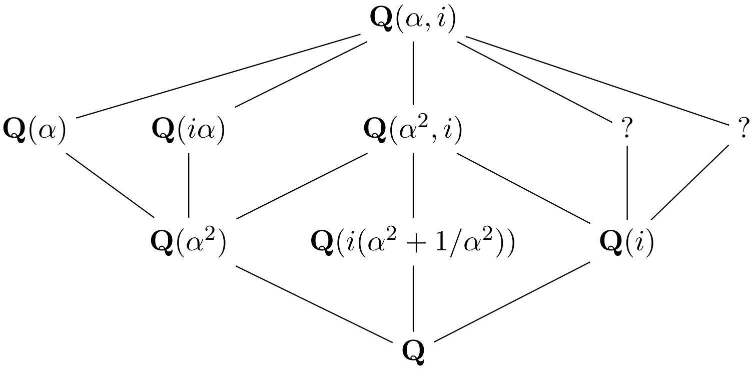


The field fixed by s is a real subfield of $\mathbf{Q}(\alpha, i)$ whose degree over $\mathbf{Q}$ is $8/2 = 4$. This field must be $\mathbf{Q}(\alpha)$, since it has degree 4 and is real. By Table 3, i is fixed by $\{1, r^2, rs, r^2 s\} = \langle r^2, rs\rangle$, so the field fixed by $\langle r^2, rs\rangle$, which must be quadratic, is $\mathbf{Q}(i)$. From the diagram of subgroups of D_4, there is a unique quadratic subfield of $\mathbf{Q}(\alpha)$ on account of there being a unique subgroup of D_4 containing $\langle s\rangle$ with index 2, namely $\langle r^2, s\rangle$. A quadratic subfield of $\mathbf{Q}(\alpha)$ is $\mathbf{Q}(\alpha^2) = \mathbf{Q}((1+\sqrt{5})/2) = \mathbf{Q}(\sqrt{5})$, so this is the fixed field of $\langle r^2, s\rangle$.

Here is a diagram of subfields of $\mathbf{Q}(\alpha, i)$ so far.



Using Table 3, $i\alpha$ is fixed by $r^2 s$, and $i\alpha$ has degree 4 over $\mathbf{Q}$ (it's a root of $X^4 + X^2 - 1$, which is irreducible mod 3 and thus irreducible over $\mathbf{Q}$). Here is a more filled-in subfield diagram. Check for each number listed in the diagram that its fixed group is the corresponding subgroup in the subgroup diagram for D_4.



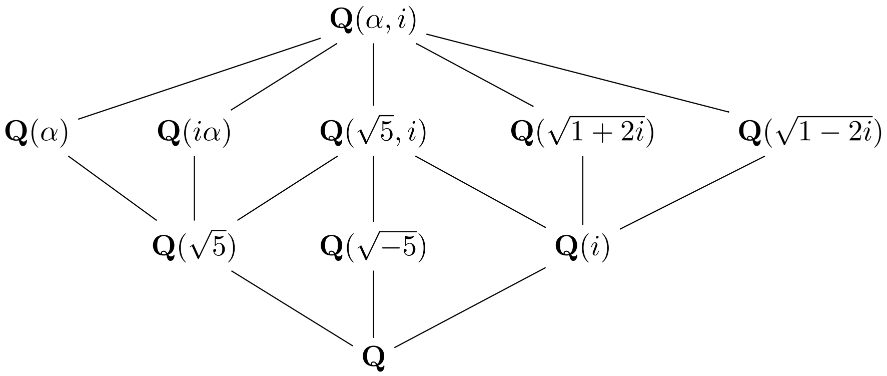
Remark 6. While the quadratic subfields of $\mathbf{Q}(\sqrt{2}, i)$ in Example 4 are $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(i)$, and $\mathbf{Q}(i\sqrt{2})$, the quadratic subfields of $\mathbf{Q}(\alpha^2, i)$ include $\mathbf{Q}(\alpha^2)$ and $\mathbf{Q}(i)$ but *not* $\mathbf{Q}(i\alpha^2)$ because $i\alpha^2$ does not have degree 2 over $\mathbf{Q}$: it has degree 4 over $\mathbf{Q}$ with minimal polynomial T^4+3T^2+1. The difference between $\sqrt{2}$ in Example 4 and $\alpha^2 = (1+\sqrt{5})/2$ in this example is that α^2 is not a pure square root of an integer, so $i\alpha^2$ need not be quadratic over $\mathbf{Q}$.

To complete the field diagram we seek elements of degree 4 over $\mathbf{Q}$ that are fixed by rs and r^3s. Since both of these automorphisms have order 2, it's natural to consider $\alpha + (rs)(\alpha) = \alpha + i/\alpha$ and $\alpha + (r^3s)(\alpha) = \alpha - i/\alpha$. To prove $\alpha + i/\alpha$ generates the fixed field of rs, let's use the field diagram: $\mathbf{Q}(\alpha + i/\alpha)$ is inside the fixed field of rs, so if it does not have degree 4 over $\mathbf{Q}$ then this field is inside $\mathbf{Q}(i)$ and thus is fixed by r^2. Since $r^2(\alpha + i/\alpha) = -\alpha - i/\alpha = -(\alpha + i/\alpha)$, the only way $\alpha + i/\alpha$ can be fixed by r^2 is if it is 0, but this would be absurd since α is a real number. So the first question mark in the above diagram is $\mathbf{Q}(\alpha + i/\alpha)$. In a similar way, the field fixed by r^3s is $\mathbf{Q}(\alpha - i/\alpha)$.

We can make the generator for the field $\mathbf{Q}(\alpha+i/\alpha)$ more explicit. Since $\alpha = \sqrt{(1+\sqrt{5})/2}$, by direct calculation

$$\left(\alpha + \frac{i}{\alpha}\right)^2 = \alpha^2 + 2i - \frac{1}{\alpha^2} = \frac{1+\sqrt{5}}{2} + 2i - \frac{\sqrt{5}-1}{2} = 1 + 2i,$$

and likewise $(\alpha - i/\alpha)^2 = 1 - 2i$. Therefore $\mathbf{Q}(\alpha + i/\alpha) = \mathbf{Q}(\sqrt{1+2i})$ and $\mathbf{Q}(\alpha - i/\alpha) = \mathbf{Q}(\sqrt{1-2i})$. Here is the field diagram with more explicit generators of the fields.



Galois theory tells us that $\mathbf{Q}(\sqrt{1+2i}) \neq \mathbf{Q}(\sqrt{1-2i})$ because these fields correspond to different subgroups of $\mathrm{Gal}(\mathbf{Q}(\alpha, i)/\mathbf{Q})$. Since $s(\alpha + i/\alpha) = \alpha - i/\alpha$, the field $\mathbf{Q}(\sqrt{1+2i})$ is carried over to $\mathbf{Q}(\sqrt{1-2i})$ by complex conjugation.