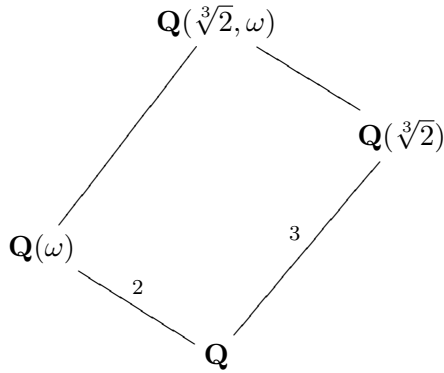


SOME EXAMPLES OF THE GALOIS CORRESPONDENCE

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 any 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 $\text{Gal}(\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q})$.



For the first way, each σ in $\text{Gal}(\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q})$ is determined by its effect on the 3 roots of $X^3 - 2$, which are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, and $\omega^2\sqrt[3]{2}$, since these roots generate the top field over the bottom field (note $\omega = \omega^3\sqrt[3]{2}/\sqrt[3]{2}$ 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 every permutation of the roots comes from an automorphism of the field extension. Therefore $\text{Gal}(\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q}) \cong S_3$ 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: any 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

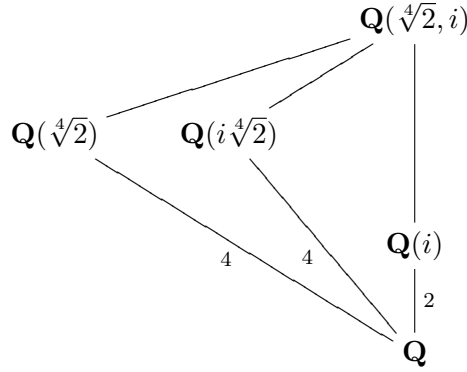
$$\sigma(\tau(\sqrt[3]{2})) = \sigma(\omega^{b_\tau}\sqrt[3]{2}) = \sigma(\omega)^{b_\tau}\sigma(\sqrt[3]{2}) = \omega^{a_\sigma b_\tau}\omega^{b_\sigma}\sqrt[3]{2} = \omega^{a_\sigma b_\tau + b_\sigma}\sqrt[3]{2}.$$

Looking at the exponents of ω on the right side of these two equations, composition of σ and τ behaves like multiplication of matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ with entries in $\mathbf{Z}/(3)$, since $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} =$

$(\begin{smallmatrix} aa' & ab'+b \\ 0 & 1 \end{smallmatrix})$: $\text{Gal}(\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q})$ is isomorphic to the group of mod 3 invertible matrices $(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix})$ by $\sigma \mapsto (\begin{smallmatrix} a_\sigma & b_\sigma \\ 0 & 1 \end{smallmatrix})$.

That we found two different models for $\text{Gal}(\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q})$, as permutations and as matrices, is no surprise since both of those groups are nonabelian and any two nonabelian groups of size 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.



Although any element of $\text{Gal}(\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q})$ 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 $\text{Gal}(\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q})$!) For example, $\sqrt[4]{2}$ and $-\sqrt[4]{2}$ add to 0, so under a field automorphism these two roots go to roots which 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 $x + y = 0$ which holds for $x = \sqrt[4]{2}$ and $y = -\sqrt[4]{2}$.

To figure out what $\text{Gal}(\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q})$ 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 $[\mathbf{Q}(\sqrt[4]{2}, i) : \mathbf{Q}] = 8$, $\text{Gal}(\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q})$ 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 $r^4 = \text{id}$, $s^2 = \text{id}$, and $rs = sr^{-1}$, so $\text{Gal}(\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q})$ 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

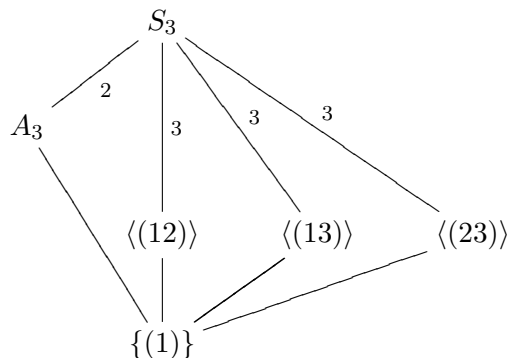
$$\alpha = \sqrt[4]{2} + \sqrt{2} + 1.$$

Applying $\text{Gal}(\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q})$ 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

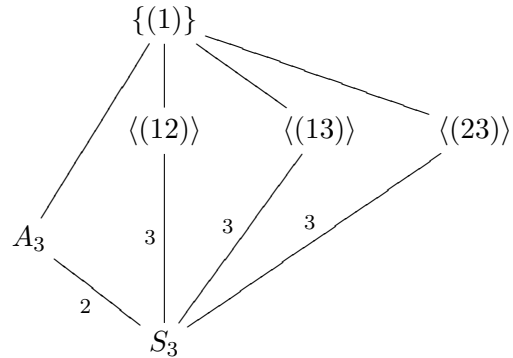
$$\sqrt[4]{2} + \sqrt{2} + 1, \quad i\sqrt[4]{2} - \sqrt{2} + 1, \quad -\sqrt[4]{2} + \sqrt{2} + 1, \quad -i\sqrt[4]{2} - \sqrt{2} + 1.$$

Although $\text{Gal}(\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q})$ 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 .

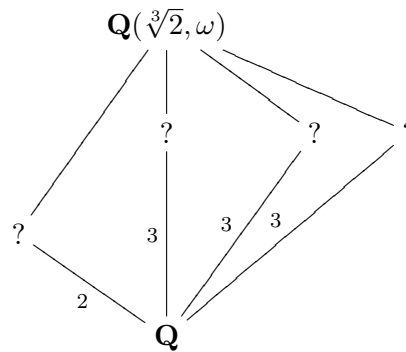
Example 3. The extension $\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q}$ has Galois group isomorphic to S_3 (Example 1). This group has 3 subgroups of order 2 and one subgroup (just A_3) of order 3. In the diagram we have indicated the indices in S_3 of subgroups.



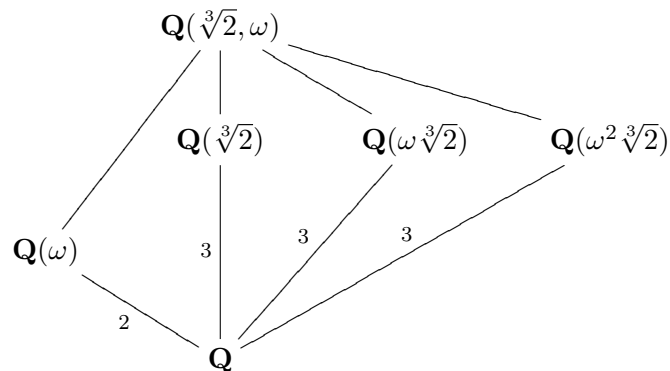
Let's flip this upside down, so larger groups are on the bottom.



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} .

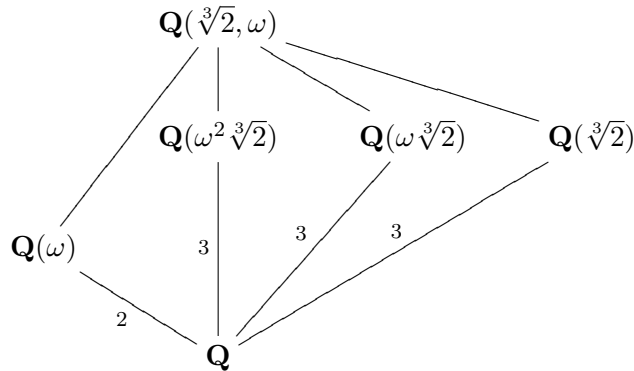
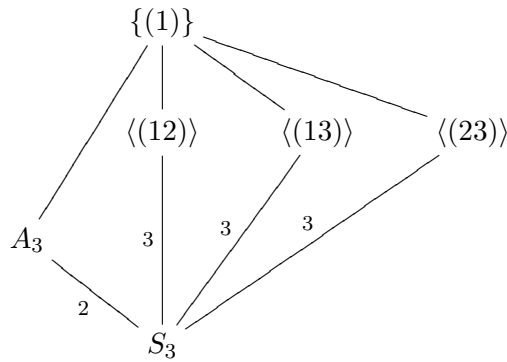


So there is one quadratic subfield and three cubic subfields. It is easy to write down enough such fields by inspection: $\mathbf{Q}(\omega)$ is quadratic and $\mathbf{Q}(\sqrt[3]{2})$, $\mathbf{Q}(\omega\sqrt[3]{2})$, and $\mathbf{Q}(\omega^2\sqrt[3]{2})$ are all cubic. (These three cubic fields are 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:



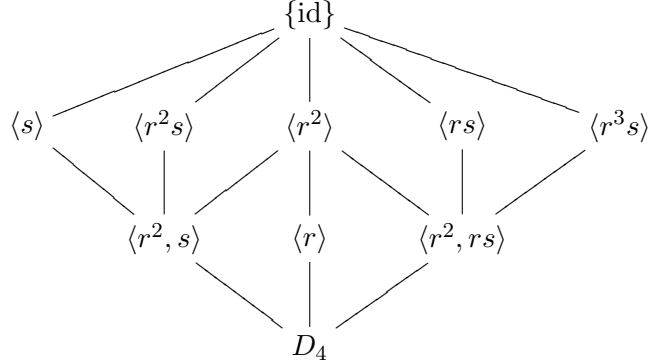
We were somewhat cavalier about the way we just wrote down the cubic fields without really paying attention to which ones should correspond to which subgroups of index 3 (order 2) in the Galois group. But we can't be more careful at this stage (beyond keeping track of indices of subgroups and degrees of subfields) because we didn't really keep track here of *how* $\text{Gal}(\mathbf{Q}(\sqrt[3]{2}, \omega)/\mathbf{Q})$ 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:

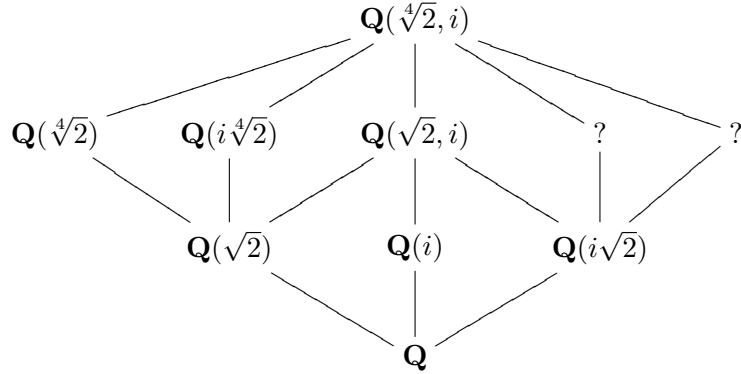


Example 4. The extension $\mathbf{Q}(\sqrt[4]{2}, i)/\mathbf{Q}$ has Galois group isomorphic to D_4 according to the permutations which the Galois group induces on the fourth roots of 2. Generators are r and s where $r(\sqrt[4]{2}) = i\sqrt[4]{2}$, $r(i) = i$ and $s(\sqrt[4]{2}) = \sqrt[4]{2}$, $s(i)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



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 $F = \mathbf{Q}(\sqrt[4]{2}, i)^H$.

As an example, the subextension $\mathbf{Q}(i)/\mathbf{Q}$ has degree 2, so its corresponding subgroup H in D_4 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 $\langle r \rangle$.

We have left two fields undetermined in the field diagram. They correspond to the subgroups $\langle rs \rangle$ and $\langle r^3 s \rangle$. The smallest subgroup properly containing either of these is $\langle r^2, rs \rangle$, so we can figure out what the undetermined fields are by looking for $\alpha \in \mathbf{Q}(\sqrt[4]{2}, i)$ of degree 4 over \mathbf{Q} that is fixed by rs and not by r^2 , and likewise find 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 out a general element of $\mathbf{Q}(\sqrt[4]{2}, i)$ in a basis over \mathbf{Q} and see what the condition $rs(\alpha) = \alpha$ means about the coefficients. Writing

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

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

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

so

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

Therefore

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

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

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

Easily $r^2(\alpha) = -\alpha$, 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 not inside the fixed field of $\langle r^2 \rangle$, so $\mathbf{Q}(\alpha)$ must be the fixed field of $\langle rs \rangle$. The difference $\beta = \sqrt[4]{2} - i\sqrt[4]{2}$ is fixed by r^3s and not by r^2 , so the fixed field of $\langle r^3s \rangle$ is $(1 - i)\sqrt[4]{2}$. Now we have a complete field diagram.

