$$\sigma^7 : \begin{cases} \theta \mapsto \zeta^3\theta \\ i \mapsto i \\ \zeta \mapsto -\zeta \end{cases} \qquad \tau\sigma^7 : \begin{cases} \theta \mapsto \zeta^5\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^3. \end{cases}$$

Since this exhausts the possibilities, these elements (together with 1 and $\tau$) are the Galois group. We see in particular that $\sigma$ and $\tau$ generate the Galois group. To determine the relations satisfied by these elements, we observe first that clearly $\tau^2 = 1$ and $(\sigma^4)^2 = 1$, so that

$$\sigma^8 = \tau^2 = 1.$$

Also, we compute

$$\sigma\tau : \begin{cases} \theta \mapsto \zeta\theta \\ i \mapsto -i \\ \zeta \mapsto \zeta^3 \end{cases}$$

so that

$$\sigma\tau = \tau\sigma^3.$$

It is not too difficult to show that these relations define the group completely, i.e.,

$$\mathrm{Gal}(\mathbb{Q}(\sqrt[8]{2}, i)/\mathbb{Q}) = \langle\ \sigma, \tau \mid \sigma^8 = \tau^2 = 1, \sigma\tau = \tau\sigma^3\ \rangle.$$

Such a group is called a *quasidihedral group* (recall that the dihedral group of order 16 would have the relation $\sigma\tau = \tau\sigma^7$ instead of $\sigma\tau = \tau\sigma^3$) and is a subgroup of $S_8$ since the Galois group is a subgroup of the permutations of the 8 roots of $x^8 - 2$.

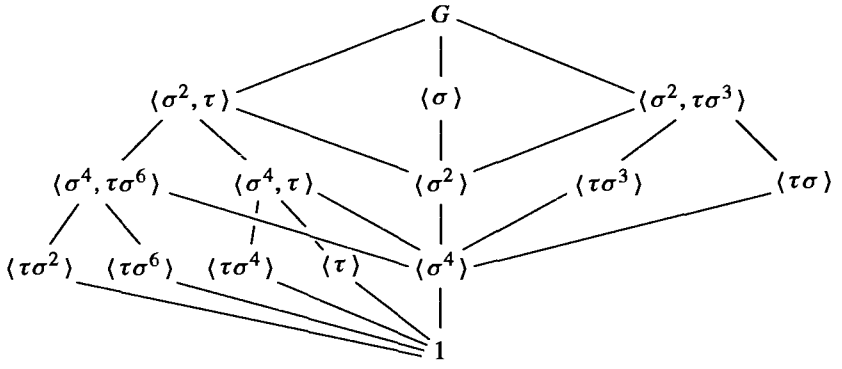
This example again illustrates that one must take care in determining Galois groups from the actions on generators. We first computed the degree of the Galois extension above to determine the number of elements in the Galois group. Had we proceeded directly from the original generators $\theta = \sqrt[8]{2}$ and $\zeta = \zeta_8$ we might have (incorrectly) concluded that there were a total of 32 elements in the Galois group, since the first generator is mapped to any of 8 possible roots of $x^8 - 2$ and the second generator is mapped to any of 4 possible roots of its minimal polynomial $\Phi_4(x) = x^4 + 1$. The problem, as previously indicated, is that these choices are not independent. Here the reason is provided by the algebraic relation

$$\theta^4 = \sqrt{2} = \zeta + \zeta^7$$

which shows that one cannot specify the images of $\theta$ and $\zeta$ independently — their images must again satisfy this algebraic relation. This relation is perhaps sufficiently subtle to serve as a caution against rashly concluding maps are automorphisms. We note that in general it is necessary to provide justification that maps are automorphisms. This can be accomplished for example by using the extension theorems or by using degree considerations as we did here.

Determining the lattice of subgroups of this group $G$ is a straightforward problem.

The lattice is the following:




Determining the subfields corresponding to these subgroups (which by the Fundamental Theorem gives *all* the subfields of $\mathbb{Q}(\sqrt[8]{2}, i)$) is quite simple for a number of the subgroups above using (2) of the Fundamental Theorem, which states that the degree of the extension over $\mathbb{Q}$ is equal to the *index* of the fixing subgroup. It then suffices to find a subfield of the right degree which is fixed by the subgroup in question. Remember also that if a subfield is fixed by the *generators* of a subgroup, then it is fixed by the subgroup. For example, from the explicit description for the automorphism $\sigma$ we see that $\mathbb{Q}(i)$ is fixed by the group generated by $\sigma$. Since this is a subgroup of index 2 and $\mathbb{Q}(i)$ is of degree 2 over $\mathbb{Q}$, it must be the full fixed field. Most of the fixed fields for the subgroups above can be determined in as simple a manner.

For the subgroups of order 4 on the right (namely, generated by $\tau\sigma^3$ and by $\tau\sigma$), it is perhaps not so easy to see how to determine the corresponding fixed field. For the subgroup $H$ generated by $\tau\sigma^3$ we may proceed as follows: the element $\theta^2 = \sqrt[4]{2}$ is clearly fixed by $\sigma^4$. By the diagram above, $\sigma^4$ is a normal subgroup of $H$ of index 2, with representatives $1, \tau\sigma^3$ for the cosets. Consider the element

$$\alpha = (1 + \tau\sigma^3)\theta^2 = \theta^2 + \tau\sigma^3\theta^2.$$

Then $\alpha$ is fixed by $\sigma^4$ (we are in a commutative group $H$ of order 4, so $\sigma^4$ commutes with 1 and $\tau\sigma^3$ and we already know $\theta^2$ is fixed by $\sigma^4$). But (and this is the point), $\alpha$ is also fixed by $\tau\sigma^3$:

$$\begin{aligned}\tau\sigma^3\alpha &= \tau\sigma^3(1 + \tau\sigma^3)\theta^2 = [\tau\sigma^3 + (\tau\sigma^3)^2]\theta^2 \\ &= (\tau\sigma^3 + \sigma^4)\theta^2\end{aligned}$$

and the last expression is just $\alpha$ since $\sigma^4\theta^2 = \theta^2$. Hence $\alpha$ is an element of the fixed field for $H$. Explicitly

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

A quick check shows that $\alpha$ is not fixed by the automorphism $\sigma^2$, so by the diagram of subgroups above, it follows that the fixing subgroup for the field $\mathbb{Q}(\alpha)$ is no larger than $H$, hence is precisely $H$, which gives us our fixed field. This also gives the fixed field for $\langle \tau\sigma \rangle$ by recalling that in general if $E$ is the fixed field of $H$ then the fixed field of $\tau H \tau^{-1}$ is the field $\tau(E)$. For $H = \langle \tau\sigma^3 \rangle$, $\tau H \tau^{-1} = \langle \tau\sigma \rangle$, with fixed field given by $\tau(\alpha) = (1 - i)\sqrt[4]{2}$.

In general one tries to determine elements which are fixed by a given subgroup $H$ of the Galois group (cf. the exercises, which indicate where the element above arose) and

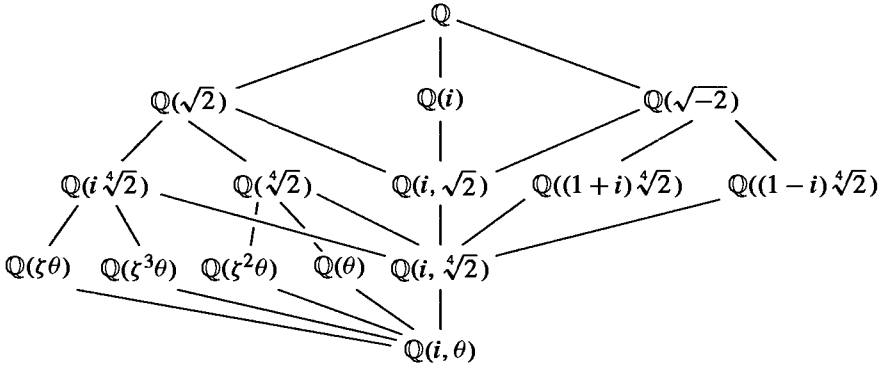
attempts to generate a sufficiently large field to give the full fixed field. In our case we were able to accomplish this with a single generator. We shall see later that every finite extension of $\mathbb{Q}$ is a simple extension, so there will be a single generator of this type, but in general it may be difficult to produce it directly.

The element $\alpha$ is a root of the polynomial

$$x^4 + 8$$

which must therefore be irreducible since we have already determined that a root of this polynomial generates an extension of degree 4 over $\mathbb{Q}$.

In a similar way it is possible to complete the diagram of subfields of $\mathbb{Q}(\sqrt[8]{2}, i)$, which we have inverted to emphasize its relation with the subgroup diagram above ($\theta = \sqrt[8]{2}$):




Note that the group $\langle \sigma^4 \rangle$ is normal in $G$ (in fact it is the center of $G$) with quotient $G/\langle \sigma^4 \rangle \cong D_8$, so the corresponding fixed field $\mathbb{Q}(i, \sqrt[4]{2})$ is Galois over $\mathbb{Q}$ with $D_8$ as Galois group. Being Galois it is a splitting field, evidently the splitting field for $x^4 - 2$. The lattice of subfields for this field is then immediate from the lattice above.

We end this example with the following amusing aspect of this Galois extension. It is an easy exercise to verify that

$$\langle \sigma^2, \tau \rangle \cong D_8 \quad \langle \sigma \rangle \cong \mathbb{Z}/8\mathbb{Z} \quad \langle \sigma^2, \tau\sigma^3 \rangle \cong Q_8$$

where $D_8$ is the dihedral group of order 8 and $Q_8$ is the quaternion group of order 8. It follows that the field $\mathbb{Q}(\sqrt[8]{2}, i)$ is Galois of degree 8 over its three quadratic subfields

$$\mathbb{Q}(\sqrt{2}) \qquad \mathbb{Q}(i) \qquad \mathbb{Q}(\sqrt{-2})$$

with dihedral, cyclic and quaternion Galois groups, respectively, so that three of the 5 possible groups of order 8 (and both non-abelian ones) appear as Galois groups in this extension.

We shall consider additional examples and applications in the following sections.

## EXERCISES

1. Determine the minimal polynomial over $\mathbb{Q}$ for the element $\sqrt{2} + \sqrt{5}$.
2. Determine the minimal polynomial over $\mathbb{Q}$ for the element $1 + \sqrt[3]{2} + \sqrt[3]{4}$.
3. Determine the Galois group of $(x^2 - 2)(x^2 - 3)(x^2 - 5)$. Determine *all* the subfields of the splitting field of this polynomial.

4. Let $p$ be a prime. Determine the elements of the Galois group of $x^p - 2$.
5. Prove that the Galois group of $x^p - 2$ for $p$ a prime is isomorphic to the group of matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ where $a, b \in \mathbb{F}_p$, $a \neq 0$.
6. Let $K = \mathbb{Q}(\sqrt[8]{2}, i)$ and let $F_1 = \mathbb{Q}(i)$, $F_2 = \mathbb{Q}(\sqrt{2})$, $F_3 = \mathbb{Q}(\sqrt{-2})$. Prove that $\mathrm{Gal}(K/F_1) \cong Z_8$, $\mathrm{Gal}(K/F_2) \cong D_8$, $\mathrm{Gal}(K/F_3) \cong Q_8$.
7. Determine all the subfields of the splitting field of $x^8 - 2$ which are Galois over $\mathbb{Q}$.
8. Suppose $K$ is a Galois extension of $F$ of degree $p^n$ for some prime $p$ and some $n \geq 1$. Show there are Galois extensions of $F$ contained in $K$ of degrees $p$ and $p^{n-1}$.
9. Give an example of fields $F_1$, $F_2$, $F_3$ with $\mathbb{Q} \subset F_1 \subset F_2 \subset F_3$, $[F_3 : \mathbb{Q}] = 8$ and each field is Galois over all its subfields with the exception that $F_2$ is not Galois over $\mathbb{Q}$.
10. Determine the Galois group of the splitting field over $\mathbb{Q}$ of $x^8 - 3$.
11. Suppose $f(x) \in \mathbb{Z}[x]$ is an irreducible quartic whose splitting field has Galois group $S_4$ over $\mathbb{Q}$ (there are many such quartics, cf. Section 6). Let $\theta$ be a root of $f(x)$ and set $K = \mathbb{Q}(\theta)$. Prove that $K$ is an extension of $\mathbb{Q}$ of degree 4 which has no proper subfields. Are there any Galois extensions of $\mathbb{Q}$ of degree 4 with no proper subfields?
12. Determine the Galois group of the splitting field over $\mathbb{Q}$ of $x^4 - 14x^2 + 9$.
13. Prove that if the Galois group of the splitting field of a cubic over $\mathbb{Q}$ is the cyclic group of order 3 then all the roots of the cubic are real.
14. Show that $\mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a cyclic quartic field, i.e., is a Galois extension of degree 4 with cyclic Galois group.
15. (*Biquadratic Extensions*) Let $F$ be a field of characteristic $\neq 2$.
    (a) If $K = F(\sqrt{D_1}, \sqrt{D_2})$ where $D_1, D_2 \in F$ have the property that none of $D_1$, $D_2$ or $D_1 D_2$ is a square in $F$, prove that $K/F$ is a Galois extension with $\mathrm{Gal}(K/F)$ isomorphic to the Klein 4-group.
    (b) Conversely, suppose $K/F$ is a Galois extension with $\mathrm{Gal}(K/F)$ isomorphic to the Klein 4-group. Prove that $K = F(\sqrt{D_1}, \sqrt{D_2})$ where $D_1, D_2 \in F$ have the property that none of $D_1$, $D_2$ or $D_1 D_2$ is a square in $F$.
16. (a) Prove that $x^4 - 2x^2 - 2$ is irreducible over $\mathbb{Q}$.
    (b) Show the roots of this quartic are

$$\alpha_1 = \sqrt{1+\sqrt{3}} \qquad \alpha_3 = -\sqrt{1+\sqrt{3}}$$
$$\alpha_2 = \sqrt{1-\sqrt{3}} \qquad \alpha_4 = -\sqrt{1-\sqrt{3}}.$$

    (c) Let $K_1 = \mathbb{Q}(\alpha_1)$ and $K_2 = \mathbb{Q}(\alpha_2)$. Show that $K_1 \neq K_2$, and $K_1 \cap K_2 = \mathbb{Q}(\sqrt{3}) = F$.
    (d) Prove that $K_1$, $K_2$ and $K_1 K_2$ are Galois over $F$ with $\mathrm{Gal}(K_1 K_2/F)$ the Klein 4-group. Write out the elements of $\mathrm{Gal}(K_1 K_2/F)$ explicitly. Determine all the subgroups of the Galois group and give their corresponding fixed subfields of $K_1 K_2$ containing $F$.
    (e) Prove that the splitting field of $x^4 - 2x^2 - 2$ over $\mathbb{Q}$ is of degree 8 with dihedral Galois group.

The following two exercises indicate one method for constructing elements in subfields of a given field and are quite useful in many computations.

17. Let $K/F$ be any finite extension and let $\alpha \in K$. Let $L$ be a Galois extension of $F$ containing $K$ and let $H \leq \mathrm{Gal}(L/F)$ be the subgroup corresponding to $K$. Define the *norm* of $\alpha$ from