A GALOIS THEORY EXAMPLE

BRIAN OSSERMAN

Let F be the splitting field of $x^4 - 2$ over $\mathbb{Q}$. This is normal because it is a splitting field, and separable because we are in characteristic 0. We compute the Galois group and all intermediate subfields. First let α be the positive, real 4th root of 2, and next observe that the roots of $x^4 - 2$ are precisely α, $-\alpha$, $i\alpha$, $-i\alpha$. It follows that $F = \mathbb{Q}(\alpha, i)$, and we also easily see that $x^4 - 2$ is irreducible over $\mathbb{Q}$, since no root is in $\mathbb{Q}$, and no product of two roots is in $\mathbb{Q}$. Thus, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Furthermore, because $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, it does not contain i, so since i is a root of quadratic polynomial (over $\mathbb{Q}$ and also over $\mathbb{Q}(\alpha)$), the field $\mathbb{Q}(\alpha, i)$ must have degee 2 over $\mathbb{Q}(\alpha)$. We conclude that $[F : \mathbb{Q}] = 8$, so $\mathrm{Gal}(F/\mathbb{Q})$ has order 8.

Now, every element of $\mathrm{Gal}(F/\mathbb{Q})$ must permute the roots of $x^4 - 2$. Furthermore, since F is the splitting field of this polynomial, it is by definition generated by its roots, so we have that $\mathrm{Gal}(F/\mathbb{Q})$ is a subgroup of the group of permutations of the roots of $x^4 - 2$. If we label the roots in the order $\alpha, -\alpha, i\alpha, -i\alpha$, we can consider $\mathrm{Gal}(F/\mathbb{Q}) \subseteq S_4$. Complex conjugation holds α and $-\alpha$ fixed, and permutes $i\alpha$ and $-i\alpha$, so under our labeling it corresponds to the transposition $g = (3, 4)$. Next, we observe that α and i are independent generators, in the sense that the relations they satisfy are generated by $\alpha^4 - 2 = 0$ and $i^2 + 1 = 0$. Thus, we can map α to any other root of $x^2 - 2$ and i to itself or $-i$, and we will obtain a unique automorphism of F. In particular, there is an automorphism of F which holds i fixed, and maps α to $i\alpha$. Under our labeling, this corresponds to the permutation $h = (1, 3, 2, 4)$. Now, it is easily verified that $ghg = h^{-1}$, so g, h generate the dihedral group of order 8, and this must be the Galois group.

The nontrivial subgroups are then the cyclic subgroups generated by h, by h^2, by g, by gh, by gh^2, and by gh^3, as well as the subgroups (each isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$) generated by gh, h^2 and by g, h^2. The lattice of subgroups is as follows:

$$\begin{tikzcd}
 & & G = \langle g, h\rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & & \\
 & \langle g, h^2\rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \langle h\rangle \arrow[d, dash] & \langle gh, h^2\rangle \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle g\rangle \arrow[drr, dash] & \langle gh^2\rangle \arrow[dr, dash] & \langle h^2\rangle \arrow[d, dash] & \langle gh\rangle \arrow[dl, dash] & \langle gh^3\rangle \arrow[dll, dash] \\
 & & \langle e\rangle & &
\end{tikzcd}$$

The subgroup generated by h has order 4, so the corresponding fixed field must have degree $8/4 = 2$ over $\mathbb{Q}$, and must contain $\mathbb{Q}(i)$, so it is equal to $\mathbb{Q}(i)$. Next, h^2 sends α to $-\alpha$ and $i\alpha$ to $-i\alpha$, so it fixes α^2 (the positive square root of 2), and since the fixed field must have degree $8/2 = 4$ over $\mathbb{Q}$, we see that the fixed field is $\mathbb{Q}(i, \sqrt{2})$. Now, g fixes α, and the fixed field has degree $8/2 = 4$ over $\mathbb{Q}$, so it must be $\mathbb{Q}(\alpha)$.

Next, gh has order 2, and sends α to $-i\alpha$ while sending i to $-i$. The fixed field has degree $8/2 = 4$ over $\mathbb{Q}$, and contains $\alpha - i\alpha$. One checks that this is not the root of any quadratic polynomial, so it generates a quartic extension which is necessarily the fixed field. Similarly, the fixed field of the group generated by gh^3 is generated by $\alpha + i\alpha$. The fixed field of the group generated by gh^2 is generated by $i\alpha$.

We then have that the fixed field of the group generated by g, h^2 is the intersection of the fixed fields for g and for h^2, which were $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(i, \sqrt{2})$, respectively. The intersection of these is $\mathbb{Q}(\sqrt{2})$. Similarly, the fixed field of group generated by gh, h^2 is the intersection of $\mathbb{Q}(\alpha - i\alpha)$ with $\mathbb{Q}(i, \sqrt{2})$, and noting that $(\alpha - i\alpha)^2 = \sqrt{2}(1 - 2i - 1) = 2i\sqrt{2}$, we see that $i\sqrt{2}$ is in both fields, so the desired fixed field must be $\mathbb{Q}(i\sqrt{2})$. We thus obtain the lattice of subfields as follows (where we have mirrored everything from top to bottom in comparing to the lattice of subgroups):

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