# M3P11 (and M4P11, M5P11) Galois Theory, Solutions to Worksheet 3

Alessio Corti

28th April 2020

**Q 1.** Write $K = \mathbb{Q}(\sqrt{2}, \sqrt{-3}, \sqrt[3]{5})$. Observe that

$$X^3 - 5 = (x - \sqrt[3]{5})(x - \omega\sqrt[3]{5})(x - \omega^2\sqrt[3]{5})$$

where

$$\omega = \frac{-1 + \sqrt{-3}}{2}$$

is a primitive cube root of unity. It follows from this that $K$ is the splitting field of the polynomial

$$f(X) = (X^2 - 2)(X^3 - 5) \in \mathbb{Q}[X]$$

indeed the polynomial splits completely in $K$ and $K$ is generated by the roots (if $\sqrt[3]{5}$ and $\omega\sqrt[3]{5}$ are both in $F$, then clearly $\omega$ is also in $F$). Hence $\mathbb{Q} \subset L$ is a normal extension.

Now let us count degrees. First, let us state that $\sqrt{2} \notin \mathbb{Q}$, hence $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Next consider the field $L = \mathbb{Q}(\sqrt{-3}, \sqrt{2})$. It is clear that, say, $\sqrt{-3} \notin \mathbb{Q}(\sqrt{2})$—for example, $\sqrt{-3}$ is purely imaginary while $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$. If you don't like this, suppose for a contradiction that $\sqrt{-3} \in \mathbb{Q}(\sqrt{2})$, that is there exist rational numbers $x, y \in \mathbb{Q}$ such that

$$-3 = (x + y\sqrt{2})^2 = x^2 + 2y^2 + 2xy\sqrt{2}$$

since this is an identity in a 2-dimensional vector space over $\mathbb{Q}$ with basis $1, \sqrt{2}$ we must have either $x = 0$ or $y = 0$. If $y = 0$, then $x^2 = -3$, $x \in \mathbb{Q}$ leads easily to a contradiction. If $x = 0$ then $-3 = 2y^2$. Writing $y = p/q$ with $p$, $q$ coprime integers, we have

$$-3q^2 = 2p^2$$

and we easily get a contradiction working $2-$ or $3-$adically.[1] By a simple application of the tower law then $[L : \mathbb{Q}] = 4$.

[1] I am deliberately avoiding reaching a contradiction by means of the order structure of the rationals: the left hand side is negative, the right hand side is positive. This would be reproducing the argument in terms of imaginary numbers that we wanted to avoid.

Finally let us consider our field $K = L(\sqrt[3]{5})$ and the diagram of field extensions:

$$\begin{tikzcd}
& K & \\
L \arrow[ur] & & \mathbb{Q}(\sqrt[3]{5}) \arrow[ul] \\
& \mathbb{Q} \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

I claim that $x^3 - 5$ is irreducible in $L[X]$ and hence $[K : L] = 3$ and then $[K : \mathbb{Q}] = [K : L][L : \mathbb{Q}] = 3 \times 4 = 12$. Indeed if $x^3 - 5$ were not irreducible in $L[X]$ then it would have a root $\alpha \in L$; and then from $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset L$ we would conclude from the tower law that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ divides $[L : \mathbb{Q}] = 4$, a contradiction. Hence $[K : \mathbb{Q}] = 12$.

**Q 2.** (i) $\mathbb{Q}(\sqrt{6})$ is the splitting field of the polynomial $x^2 - 6$ and is hence normal over $\mathbb{Q}$.

(ii) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $(x^2 - 2)(x^2 - 3)$ and is hence normal.

(iii) $\mathbb{Q}(7^{1/3})$ contains one, but not all, roots of the irreducible polynomial $x^3 - 7$ (because the other roots are not even real), so it is not normal over $\mathbb{Q}$.

(iv) $\mathbb{Q}(7^{1/3}, e^{2\pi i/3})$ is the splitting field of $x^3 - 7$ and is hence normal.

(v) $\mathbb{Q}(\sqrt{1 + \sqrt{7}})$ is not normal over $\mathbb{Q}$. Here's why. If $\alpha = \sqrt{1 + \sqrt{7}}$ then $\alpha^2 - 1 = \sqrt{7}$, so $(\alpha^2 - 1)^2 = 7$ and $\alpha$ is hence a root of $x^4 - 2x^2 - 6 = 0$. We can spot the four complex roots of this polynomial; they are $\pm\sqrt{1 \pm \sqrt{7}}$ (just substitute in to see that all of these are roots). Two of these numbers are real and two pure imaginary; in particular not all of them are in $\mathbb{Q}(\sqrt{1 + \sqrt{7}})$, which is a subfield of the reals. However, $x^4 - 2x^2 - 6 = 0$ is irreducible over $\mathbb{Q}$ (one can use the Eisenstein criterion, which I haven't done yet, or argue in an adhoc manner, or, at this point, use the theory developed in class on biquadratic extensions), so this polynomial has some but not all roots in $\mathbb{Q}(\sqrt{1 + \sqrt{7}})$ which is hence not normal over $\mathbb{Q}$.

(vi) $\mathbb{Q}(\sqrt{2 + \sqrt{2}})$ is normal over $\mathbb{Q}$, despite the formal similarity with part (v). If $\alpha = \sqrt{2 + \sqrt{2}}$ then (as in the previous question) we see $(\alpha^2 - 2)^2 = 2$ and hence $\alpha$ is a root of $x^4 - 4x^2 + 2 = 0$. This polynomial is irreducible by Eisenstein, but in this case $\mathbb{Q}(\sqrt{2 + \sqrt{2}})$ is actually its splitting field. For two of its roots are $\pm\alpha$ and the other two are $\pm\sqrt{2 - \sqrt{2}}$ and if $\beta = \sqrt{2 - \sqrt{2}}$ then we see $\alpha\beta = \sqrt{2} = \alpha^2 - 2$, and hence $\beta = (\alpha^2 - 2)/\alpha \in \mathbb{Q}(\alpha)$! So the extension is a splitting field and hence normal.

**Q 3.** (a) If $[F : E] = 2$ let $\alpha \in F \setminus E$, then consider the tower of field extensions $E \subset E(\alpha) \subset F$. As a simple consequence of the tower law we get that $F = E(\alpha)$. The minimal polynomial of $\alpha$ over $E$ has degree 2:

$$f(X) = X^2 + aX + b \in E[X]$$

and $X - \alpha$ divides $f(X)$ in $F[X]$ hence $f(X)$ splits completely in $F$, hence $F$ is the splitting field of $f(X)$ hence $E \subset F$ is a normal extension.

(b) Suppose that $H \leq G$ has index two. This means that there are two elements (cosets) in the quotient set $X = H\backslash G$ and also in the quotient set $Y = G/H$. Let $g \in G$ be any element: if $g \in H$ then clearly $g^{-1}Hg = H$, so let us assume that $g \notin H$. It must be the case that $Hg = G \setminus H$ AND $gH = G \setminus H$; therefore $Hg = gH$.[2]

**Q 4.** (i) We know $x^p - 1 = (x-1)(1+x+x^2+\cdots+x^{p-1})$, and $f(x) := 1+x+x^2+\cdots+x^{p-1}$ is irreducible over $\mathbb{Q}$ (by Eisenstein after a coordinate change). Hence if $\zeta = e^{2\pi\,\mathtt{i}/p}$ then $f(x)$ must be the min poly of $\zeta$. Note that the roots of $p(x)$ are just the roots of $x^p - 1$ other than $x = 1$, so they're $\zeta^j$ for $1 \leq j \leq p-1$. Moreover if $F = \mathbb{Q}(\zeta)$ then $[F : \mathbb{Q}] = \deg(f) = p-1$, and $K$ contains $\zeta^j$ for all $j$, so $x^p - 1$ splits completely in $K$. Hence $K$ is the splitting field of $x^p - 1$ and it has degree $p-1$.

Now $F/\mathbb{Q}$ is finite, normal and separable, so the fundamental theorem applies, so we know $\mathrm{Gal}(F/\mathbb{Q})$ will have size $p-1$. If $\tau \in \mathrm{Gal}(F/\mathbb{Q})$ then, because $F = \mathbb{Q}(\zeta)$, $\tau$ is determined by $\tau(\zeta)$, which is a root of $\tau(f) = f$, so is $\zeta^j$ for some $1 \leq j \leq p-1$. It's perhaps not immediately clear that, given $j$, some field automorphism $\tau$ of $F$ sending $\zeta$ to $\zeta^j$ will exist – but it has to exist because we know there are $p-1$ field automorphisms. So the elements of the Galois group can be called $\tau_j$ for $1 \leq j \leq p-1$. The remaining question is what this group is. We can figure out the group law thus: $\tau_i \circ \tau_j$ – where does this send $\zeta$? Well $\tau_j(\zeta) = \zeta^j$, and $\tau_i(\zeta) = \zeta^i$ so $\tau_i(\zeta^j) = \zeta^{ij}$ as $\tau_i$ is a field homomorphism. Note finally that $\zeta^{ij}$ only depends on $ij$ mod $p$, as $\zeta^p = 1$. So if we identify $\mathrm{Gal}(F/\mathbb{Q})$ with $\{1, 2, \ldots, p-1\}$ then the group law is just "multiplication mod $p$" , and we see $\mathrm{Gal}(F/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.

If you will, check that our isomorphism (which seemed to depend on a choice of $\zeta$, our $p$th root of unity) is in fact independent of that choice, so $\mathrm{Gal}(F/\mathbb{Q})$ is *canonically* isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$. The notation in mathematics for a canonical isomorphism is "=", so we can write $\mathrm{Gal}(F/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times$ in this situation. This concludes part (i). I want to add to this that, in fact, $(\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}$ is always a cyclic group. (This is a non-completely trivial fact. In general, every finite subgroup of the multiplicative group of a field is cyclic. I don't normally like to prove this result — sometimes I give it as a worksheet question — but I encourage you to look it up.)

As for part (ii), I discuss some ideas without giving a complete proof.

When $p = 3$, $K = F$ and hence $K = \mathbb{Q}(\sqrt{-3})$.

When $p = 5$, I claim that $K = \mathbb{Q}(\sqrt{5})$. Indeed from part (i) $G = (\mathbb{Z}/5\mathbb{Z})^\times = \{1, 2, -2, -1\}$. It is clear that $H = \{1, -1\} \subset G$ has index 2 and that $K = H^\star$ in the notation of the Galois correspondence. Writing as in part (i) $\zeta = e^{\frac{2\pi\,\mathtt{i}}{5}}$, it is clear that

$$\alpha = \zeta + \frac{1}{\zeta} \in H^\star$$

and it is reasonable to guess $K = \mathbb{Q}(\alpha)$. It is easy to finish from here:

$$\alpha^2 + \alpha - 1 = 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$$

hence $\alpha = \frac{-1+\sqrt{5}}{2}$ and from this we conclude that $K = \mathbb{Q}(\sqrt{5})$.

[2] You are supposed to "see" that the two parts of the question correspond under the Galois correspondence.

For $p$ general, writing as above $\zeta = e^{\frac{2\pi\mathrm{i}}{p}}$, and denoting by $H \leq (\mathbb{Z}/p\mathbb{Z})^\times$ the unique subgroup of index 2, we want to evaluate something like

$$\sum_{h\in H} h(\zeta)$$

because this thing being the average over all of $H$ is manifestly $H$-invariant. The next observation is that $H$ is the image of the "squaring homomorphism"

$$(\mathbb{Z}/p\mathbb{Z})^\times \ni k \mapsto k^2 \in (\mathbb{Z}/p\mathbb{Z})^\times$$

so we are led to evaluating:

$$\alpha = \sum_{k=0}^{\frac{p-1}{2}} e^{\frac{2\pi\mathrm{i}k^2}{p}}$$

You can find this thing in number theory books under the name of "quadratic Gauss sum" and the upshot is

$$K = \begin{cases} \mathbb{Q}(\sqrt{-p}) & \text{if } p \equiv 3 \bmod 4 \\ \mathbb{Q}(\sqrt{p}) & \text{if } p \equiv 1 \bmod 4 \end{cases}$$

(The exact evaluation of the Gauss sum is a bit tricky, but you may be able to evaluate it up to sign, and this is enough to determine $K$. This, however, is a number theory question, not a Galois theory question.)

**Q 5.** (i) $a > 1$ so $a$ has a prime divisor $p$; now use Eisenstein. Or use uniqueness of factorization to prove $\sqrt{a} \notin \mathbb{Q}$.

Next, if $\sqrt{b} \in \mathbb{Q}(\sqrt{a})$ then write $\sqrt{b} = x + y\sqrt{a}$; square, and use the fact that $\sqrt{a}$ is irrational to deduce that $2xy = 0$. Hence either $y = 0$ (contradiction, as $\sqrt{b} \notin \mathbb{Q}$) or $x = 0$ (contradiction, as we can write $ab = cd^2$ with $c$ squarefree, and $a \neq b$ so $c \neq 1$, and again $\sqrt{c} \notin \mathbb{Q}$).

(ii) $F = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ and the preceding part, plus the tower law, shows that $[F : \mathbb{Q}] = 4$. Now $F$ is a splitting field in characteristic zero, so it's finite, normal and separable. By the fundamental theorem, $\mathrm{Gal}(F/\mathbb{Q})$ must be a finite group of order 4, so it's either $C_4$ or $C_2 \times C_2$. There are lots of ways of seeing that it is actually $C_2 \times C_2$. Here are two that spring to mind: firstly, $C_4$ only has one subgroup of order 2, whereas $F$ has at least two subfields of degree 2 over $\mathbb{Q}$, namely $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{b})$, so by the correspondence in the fundamental theorem, $C_4$ is ruled out. And another way – if we set $K = \mathbb{Q}(\sqrt{a})$ then $F/K$ is normal and separable and $[F : K] = 2$, so $\mathrm{Gal}(F/K)$ is cyclic of order 2 by the fundamental theorem, and the Galois group permutes the roots of $x^2 - b$. We deduce that there must be an element of $\mathrm{Gal}(F/K)$, and thus a field automorphism $g_a$ of $F$, that sends $+\sqrt{b}$ to $-\sqrt{b}$ and fixes $\sqrt{a}$ (as it fixes $K$). Similarly there's an automorphism $g_b$ of $F$ that sends $+\sqrt{a}$ to $-\sqrt{a}$ and fixes $\sqrt{b}$. This gives us two elements of order 2 in $\mathrm{Gal}(F/\mathbb{Q})$, which must then be $C_2 \times C_2$. Of course their product, $g_a g_b$, sends $\sqrt{a}$ to $-\sqrt{a}$ and $\sqrt{b}$ to $-\sqrt{b}$, so it fixes $\sqrt{ab}$ and is the third non-trivial element of $\mathrm{Gal}(F/\mathbb{Q})$.

The subgroups of $C_2 \times C_2$ are: the subgroup of order 1 (corresponding to $F$), the group itself, of order 4 (corresponding to $\mathbb{Q}$) (both of these because the Galois correspondence is order-reversing, so i.e. sends the biggest things to the smallest things and vice-versa), and then there are three subgroups of order 2, corresponding to $\mathbb{Q}(\sqrt{a})$, $\mathbb{Q}(\sqrt{b})$ and $\mathbb{Q}(\sqrt{ab})$. One way to see this for sure is, for example, that $g_a$ fixes $\sqrt{a}$, so the subfield corresponding to $\langle g_a\rangle$ definitely contains $\sqrt{a}$, but has degree 2 over $\mathbb{Q}$ by the tower law and so must be $\mathbb{Q}(\sqrt{a})$. Arguing like this will show everything rigorously.

Finally, all of the subfields are normal over $\mathbb{Q}$, because all subgroups of $\mathrm{Gal}(F/\mathbb{Q})$ are normal (as it's abelian).

(iii) Every element of $\mathrm{Gal}(F/\mathbb{Q})$ sends $\sqrt{a}+\sqrt{b}$ to something else! (for example $g_a$ sends it to $\sqrt{a}-\sqrt{b}$). So the subgroup of $\mathrm{Gal}(F/\mathbb{Q})$ corresponding to $\mathbb{Q}(\sqrt{a}+\sqrt{b})$ must be the identity, which corresponds to $F$, and so $F=\mathbb{Q}(\sqrt{a}+\sqrt{b})$.

(iv) If $\sqrt{r}\in\mathbb{Q}(\sqrt{p},\sqrt{q})$ then $\mathbb{Q}(\sqrt{r})$ must be one of the quadratic subfields of $\mathbb{Q}(\sqrt{p},\sqrt{q})$, and hence it must be either $\mathbb{Q}(\sqrt{p})$, $\mathbb{Q}(\sqrt{q})$ or $\mathbb{Q}(\sqrt{pq})$ by part (ii). But by part (i) $\sqrt{r}$ is not in any of these fields! Done.

(v) $[F:\mathbb{Q}(\sqrt{p},\sqrt{q})]$ must be 2 (as it isn't 1) and now use the tower law. The Galois group – we know firstly that any element of the Galois group will be determined by what it does to $\sqrt{p}$, $\sqrt{q}$ and $\sqrt{r}$, and of course $\sqrt{n}$ must be sent to $\pm\sqrt{n}$ for any $n\in\mathbb{Q}$, so there are at most eight possibilities for $\mathrm{Gal}(F/\mathbb{Q})$, corresponding to the $8=2^3$ choices we have for the signs. However we know the size of $\mathrm{Gal}(F/\mathbb{Q})$ is eight, so all eight possibilities must occur and the group must be $C_2\times C_2\times C_2$.

Let me stress here, for want of a better place, that you *cannot* just say "clearly $\sqrt{p}$, $\sqrt{q}$ and $\sqrt{r}$ are "independent" so we can move them around as we please" – one really has to come up with some sort of an argument to prove that there really is a field automorphism of $F$ sending, for example, $\sqrt{p}$ to $-\sqrt{p}$, $\sqrt{q}$ to $+\sqrt{q}$ and $\sqrt{r}$ to $-\sqrt{r}$. You can build it explicitly from explicit elements you can write down in the Galois group using degree 4 subfields, or you can get it via the counting argument I just explained, but you *can't* just say "it's obvious" because Galois theory is offering you precisely the framework to make the arguments rigorous and I don't think it is obvious without this framework.

(vi) Think of the Galois group as a 3-dimensional vector space over the field with two elements. There are seven 1-dimensional subspaces (each cyclic of order 2 and generated by the seven non-trivial elements), and there are also seven 2-dimensional subspaces, by arguing for example on the dual vector space – or by arguing that any subgroup of order 4 of $C_2\times C_2\times C_2$ is the kernel of a group homomorphism to $C_2$ and such a homomorphism is determined by where the three generators go; there are eight choices, one of which gives the trivial homomorphism and the other seven of which give order 4 subgroups.

Hence other than $F$ and $\mathbb{Q}$ there are 14 fields; seven have degree 2 and seven have degree 4. The degree 2 ones are $\mathbb{Q}(\sqrt{p^aq^br^c})$ as $a,b,c$ each run through 0 and 1, but not all zero. The degree 4 ones are $\mathbb{Q}(\sqrt{p^aq^br^c},\sqrt{p^dq^er^f})$ as $(a,b,c),(d,e,f)$ run through bases of the seven 2-dimensional subspaces of the Galois group considered as a vector space of dimension 3 over the field with 2 elements.

(vii) We know all seven non-trivial elements of the Galois group, and none of them fix $\sqrt{p}+\sqrt{q}+\sqrt{r}$ (because if you think of it as a real number, they all send it to something strictly smaller), so the subgroup corresponding to $\mathbb{Q}(\sqrt{p}+\sqrt{q}+\sqrt{r})$ is trivial and we're home.

(viii) Induction and the argument in (v) gives the degree; considering possibilities of signs gives that the Galois group is what you think it is, acting how you think it acts, and the last part again follows by observing that $\mathbb{Q}(\sqrt{p_1}+\sqrt{p_2}+\cdots+\sqrt{p_n})$ corresponds to the trivial subgroup.

**Q 6.**

$$\begin{aligned}\mathbb{Q} &\subseteq \mathbb{Q}\left(8^{1/5}\right)\\ &\subseteq \mathbb{Q}\left(8^{1/5}, \sqrt{8^{1/5}+6}\right)\\ &\subseteq \mathbb{Q}\left(8^{1/5}, \sqrt{8^{1/5}+6}, 5^{1/3}\right)\\ &\subseteq \mathbb{Q}\left(8^{1/5}, \sqrt{8^{1/5}+6}, 5^{1/3}, \sqrt[11]{5^{1/3}+\sqrt{8^{1/5}+6}}\right)\\ &\subseteq \mathbb{Q}\left(8^{1/5}, \sqrt{8^{1/5}+6}, 5^{1/3}, \sqrt[11]{5^{1/3}+\sqrt{8^{1/5}+6}}, 9^{1/7}\right)\end{aligned}$$

**Q 7.** This question is not for you to literally do it but to show you what is possible. In fact the statements are very tedious to prove and not super-useful, which is why they are typically omitted from lecture courses.[3]

(a) To sow that the action is transitive is to show that given two $K$-embeddings $x, y\colon F \to L$, there exists a $K$-embedding $g\colon L \to L$ — that is to say, an element $g$ of the Galois group — such that $y = gx$. This is Question 8, part (a) below. The fact just proven generalizes the statement: Let $K$ be a field, $f(x) \in K[x]$ an *irreducible* polynomial, and $K \subset L$ the splitting field of $f(x)$. Then $G = \mathrm{Emb}_K(L, L)$ acts transitively on the roots of $f(x)$. To derive this from the abstract statement about fields, just note that roots of $f(x)$ are in one-to-one correspondence with $K$-embeddings

$$x\colon F \to L$$

where $F = K[x]/f(x)$.

The last statement is a tautology: we have an injection $i\colon F \to L$ by means of which we consider $F$ as a *subset* of $L$, i.e. the elements of $F$ are elements of $L$. For $g \in G$ to say that $gi = i$ is exactly to say that $g|F$ is the identity on $F$, in other words $g \in F^\dagger$.

(b) Suppose that $K \subset F$ is normal. Let $g \in G$, $h \in H$ and consider $g^{-1}hg$. Since $g\colon L \to L$ is a $K$-embedding, it follows that $g|F\colon F \to L$ is also a $K$-embedding, and then, because $K \subset F$ is normal, we have $g(F) \subset F$ (this is exactly our definition of normal extension of fields). So for all $a \in F$, $g(a) \in F$ and hence $h(g(a)) = g(a)$ and hence $g^{-1}hg\ (a) = a$, that is $g^{-1}hg \in F^\dagger = H$ or, in other words, $H$ is a normal subgroup of $G$.

Suppose now that $H \leq G$ is a normal subgroup. For clarity let me name $x\colon F \to L$ the given embedding. For all $g \in G$, we want to show that $gx(F) \subset x(F)$.

In general, if a group $G$ acts on a set $X$, then for all $g \in G$ and $x \in X$, $G_{gx} = gG_xg^{-1}$. What we want now follows from part (a):

$$x^\dagger = H = G_x = gG_xg^{-1} = G_{gx} = (gx)^\dagger$$

[3] I had to revise this question significantly, see v2 of the Worksheet.

therefore $F$ and $gF$ are the same field, because they have the same dagger $H$ (Galois correspondence).

Finally, if $K \subset F$ is normal, restriction gives a group homomorphism $\rho\colon G \to \mathrm{Emb}_K(F,F)$. The kernel is clearly $H$; and $\rho$ is surjective by part (a).

(c) This is a small step from (b). For any $K \subset F \subset L$ for clarity denote by $x\colon F \to L$ the given inclusion. *Claim*: For all $g \in G$, $g(F) \subset F$ if and only if $g \in N_G(H)$.

Indeed, suppose that $g(F) \subset F$. Then in fact $g(F) = F$ (an injective linear map between finite dimensional vector spaces of the same dimension is an isomorphism) and hence $(gx)^\dagger = x^\dagger$, which implies as above

$$gHg^{-1} = gG_xg^{-1} = G_{gx} = (gx)^\dagger = x^\dagger = G_x = H$$

and hence $g \in N_G(H)$. Conversely and similarly, if $gHg^{-1} = H$, then $(gx)^\dagger = x^\dagger$, hence $gx(F)$ and $x(F)$ are the same subfields of $L$, that is $g(F) = F$. This shows the claim.

From the claim it follows that restriction is a group homomorphism $\rho\colon N_G(H) \to \mathrm{Emb}_K(F,F)$; the kernel is obviously $H$ and the image is everything: if $u \in \mathrm{Emb}_K(F,F)$ then by part (a) there is $g \in G$ such that $gx = xu$, in other words $g|F = u$: by what we said earlier $g \in N_G(H)$ and by what we just said $\rho(g) = u$.

(d) This part is a minor variation on part (c). Here we start from two $K$-embeddings $x_1\colon F_1 \to L$, $x_2\colon F_2 \to L$ and set $H_1 = x_1^\dagger, H_2 = x_2^\dagger$. *Claim*: For all $g \in G$, $gx_1(F_1) \subset x_2(F_2)$ if and only if $g \in N(H_1,H_2)$. Indeed, by the Galois correspondence, $gx_1(F) \subset x_2(F)$ if and only if $(gx_1)^\dagger \supset x_2^\dagger$ if and only if $gH_1g^{-1} \supset H_2$.

From the claim we construct a restriction map

$$\rho\colon N(H_1,H_2) \to \mathrm{Emb}_K(x_1,x_2)$$

which is surjective by part (a). Suppose that $g, g' \in N(H_1,H_2)$. This just means that $gx_1 = g'x_1$ or in other words $g^{-1}g' \in H_1$.

(e) This is really pretty easy. I show the last bit: suppose that $g_1, g_2 \in N(H_1,H_2)$ and that $T_{g_1} = T_{g_2}$. This means that for all $h \in H_2$, $g_1^{-1}hg_1 = g_2^{-1}hg_2$ or, equivalently

$$g_2g_1^{-1}h = hg_2g_1^{-1}, \quad \text{that is} \quad z = g_2g_1^{-1} \in C(H_2)$$

(f) This is not hard but it is boring. The composition we are talking about is inherited from the composition of part (e). You need to check that the composition of part (e) is compatible with various equivalence relations.

(g) This is all an elaborate way to rephrase part (d).

**Q 8.** (a) By assumption $K \subset L$ (there is only one such inclusion so I don't need to call it anything) is normal, hence it is the splitting field of a polynomial $f(x) \in K[x]$; so now $x_i\colon F \to L$ is also a splitting field of $f(x)$, and the first half of part (a) (existence of $y$) follows from uniqueness of splitting fields over $F$.

(The fact that $y$ is a field automorphism follows from a familiar argument: it is injective because every field homomorphism is, and it is surjective by the rank-nullity theorem, because it is an injective $K$-linear endomorphism of a finite dimensional $K$-vector space.)

(b) Define a set-theoretic function

$$y_\star \colon \operatorname{Emb}_{x_1}(E, L) \to \operatorname{Emb}_{x_2}(E, L)$$

as follows:

$$y_\star(\widetilde{x}) = y \circ \widetilde{x}$$

Indeed, suppose that $a \in F$, then

$$y_\star(\widetilde{x})(a) = y\big(\widetilde{x}(a)\big) = y\big(x_1(a)\big) = x_2(a)$$

therefore, as claimed, $y_\star(\widetilde{x}) \in \operatorname{Emb}_{x_2}(E, L)$.

Finally $y_\star$ is a bijective correspondence because it has an inverse given by $(y^{-1})_\star$.

**Q 9.** (a) First note that if $\alpha = 2^{1/3}$ then $L$ is the splitting field of $x^3 - 2$ over $\mathbb{Q}$; indeed the splitting field is by definition $\mathbb{Q}(\alpha, \omega\alpha, \omega^2\alpha)$ (as these are the roots), and this field must be $\mathbb{Q}(\alpha, \omega)$ because each of the generators of one field can be easily checked to be in the other.

We immediately deduce that $K \subset L$ and $F \subset L$ are normal because (both are the splitting field of $X^3 - 2$, seen as a polynomial in either $K[X]$ or $F[X]$. (We can also deduce normality of $F \subset L$ from normality of $K \subset L$). However $K \subset F$ is not normal, because $x^3 - 2$ is irreducible over $K$ and has one, but not all, roots in $F$.

(b) Let's first compute some degrees. We know the min poly of $\sqrt{2}$ over $\mathbb{Q}$ has degree 2, so $[F : K] = 2$. Also the min poly of $2^{1/4}$ over $\mathbb{Q}$ must be $x^4 - 2$ (because this poly is irred by Eisenstein), and hence $[L : K] = 4$. By the tower law we deduce $[L : F] = 2$ (and hence that $x^2 - \sqrt{2}$ must be the min poly of $2^{1/4}$ over $F$, but we don't need this). We could use Question 3 to deduce that $K \subset F$ and $F \subset L$ are normal, but we could also see it directly: $F$ is the splitting field of $x^2 - 2$ over $K$ and $L$ is the splitting field of $x^2 - \sqrt{2}$ over $F$, so they're both normal. However $x^4 - 2$ is irreducible over $K$ and has one root in $L$ (in fact two roots in $L$) but not all its roots (as two are not real, whereas $L \subseteq \mathbb{R}$ so $K \subset L$ is not normal.

(c) If $H$ is normal in $G$ then $g^{-1}Hg = H$ for all $g \in H$, so trivially $g^{-1}Hg = H$ for all $g \in K$, so $H$ is normal in $K$.

Examples: $H = \{1\} \subseteq K = \langle (1\,2\rangle \subseteq S_3$ for the first, and $H = \langle\sigma\rangle \subseteq K = \langle\sigma, \rho^2\rangle \subseteq G = D_8$ for the second, with $D_8 = \langle\rho, \sigma\rangle$ the dihedral group generated by a rotation $\rho$ of order 4 and a reflection $\sigma$ of order 2.