Math 121. Fundamental Theorem and an example

Let K/k be a finite Galois extension and $G = \mathrm{Gal}(K/k)$, so $\#G = [K : k]$ by the counting criterion for separability discussed in class. In this handout we will prove the Galois correspondence relating subgroups of G to intermediate fields between K and k, and we work it out for an interesting example. (The course text works out *a lot* of examples in §14.2; I highly recommend studying those examples in order to get a sense of the techniques one can bring to bear on the task of computing Galois groups and the subgroup-subfield correspondence in explicit situations.)

The proof of the Galois correspondence in the course text uses the method of "linear independence of characters" which I find to be somewhat opaque at first sight (though it is useful in other settings). In this handout we use the more hands-on method of the Primitive Element Theorem (as in the lectures too). The reader is invited to decide which approach to the proofs they find preferable.

1. Artin's Lemma

The key to the proof is the so-called Lemma of Artin, which concerns a finite subgroup G of the automorphism group $\mathrm{Aut}(K)$ of an abstract field K. Here there is no "ground field" (though eventually we will specialize to the case $G = \mathrm{Gal}(K/k) \subset \mathrm{Aut}(K)$ for a finite Galois extension K/k). Artin's Lemma concerns the relationship between K and its subfield K^G of G-invariant elements (i.e., K^G is the set of $x \in K$ such that $g(x) = x$ for all $g \in G$; this really is a subfield, as one easily checks from the definitions). A priori it may not be clear if K is a finite extension of K^G, let alone algebraic, separable, or normal over K^G; Artin's Lemma says that these properties always hold. In fact, it gives more:

Lemma 1.1 (Artin)**.** *In the above setup, K is a finite Galois extension of K^G and the inclusion $G \subset \mathrm{Gal}(K/K^G)$ as subgroups of $\mathrm{Aut}(K)$ is an equality.*

Make sure you understand why $G \subset \mathrm{Aut}(K/K^G)$ inside $\mathrm{Aut}(K)$ using just the definition of K^G, and that it is *not* obvious why this inclusion should be an equality (let alone that K/K^G should be finite Galois). The key issue is that it isn't evident why there can't be an automorphism of K which fixes K^G pointwise yet doesn't arise from an element of G.

The proof of Artin's Lemma will be in a series of stages. First we will show K is *algebraic* over K^G, and then that it is separable and normal. Only after establishing these properties (especially separability) will we establish that $[K : K^G]$ is *finite* by a nifty application of the Primitive Element Theorem. Finally we put it all together to deduce that this finite Galois extension has G as its Galois group (and not something bigger).

Step 1: Let's show that K is algebraic over K^G. Pick $a \in K$, and consider the monic polynomial $f_a(X) = \prod_{g \in G}(X - g(a)) \in K[X]$. Note that $f(a) = 0$ due to the factor $X - a$ occuring for $g = 1$. The key point is to show that $f \in (K^G)[X]$. To see what is going on, suppose for a moment that $G = \{g_1, g_2, g_3\}$ consists of 3 elements. Then expanding the product,

$$f_a(X) = X^3 - (\sum g_i(a))X^2 + (\sum_{i<j} g_i(a)g_j(a))X - \prod g_i(a) \in K[X].$$

If we apply an element $g \in G$ to any of the coefficients, the terms of each sum or product may get shuffled around, but the actual coefficient doesn't change! Think about it for the above special case $\#G = 3$.

Informally, the coefficients of f_a are (up to sign) the elementary symmetric functions of the G-orbit of a, and applying an element of G to the G-orbit permutes terms in the sums and products defining the elementary symmetric functions but has no effect on the total value of each coefficient.

(Beware that we are *not* claiming that the list of elements $g(a)$ for $g \in G$ has no repetitions – consider the silly case when $a \in K^G$! – but for our consideration of elementary symmetric functions we're using as out indexing set the elements of G and *not* the literal values $g(a)$ which might occur with repetitions as we vary g.) This reasoning applies regardless of the size of the finite group G, so we conclude that $f_a \in (K^G)[X]$. Hence, we have exhibited an algebraic dependence of each $a \in K$ over K^G, so K is algebraic over K^G.

Step 2: Since $f_a(a) = 0$, the minimal polynomial m_a over K^G for $a \in K$ is a factor of $f_a \in (K^G)[X]$. But f_a visibly splits completely over K by the very definition of f_a (!), so any monic factor of f_a in $(K^G)[X]$ also splits completely over K. In particular, m_a splits completely over K, so K contains a splitting field over K^G for m_a for every $a \in K$. Hence, K/K^G is normal.

Now we refine the construction of f_a to see that each m_a is separable, so the algebraic extension K/K^G is also separable (not yet shown to be of finite degree). The point is to remove redundant factors in the definition of f_a. More specifically, consider the subgroup $G_a = \mathrm{Stab}_G(a)$ of elements $g \in G$ such that $g(a) = a$. (This is easily checked to be a subgroup of G.) Observe that for any $g' \in G$, the value $g'(a) \in K$ depends only on the coset $g'G_a$. Indeed, if $h \in G_a$ then $(g'h)(a) = g'(h(a)) = g'(a)$. Conversely, if $g', g'' \in G$ satisfy $g'(a) = g''(a)$ then $g'^{-1}(g''(a)) = g'^{-1}(g'(a)) = a$, which is to say $g'^{-1}g'' \in G_a$, so $g'' \in g'G_a$. In other words, for any coset $\overline{g} \in G/G_a$ and representative $g \in G$ for the coset we see that $g(a)$ only depends on $\overline{g}$ and that *as we vary* $\overline{g}$ *the elements* $g(a)$ *genuinely change* (with $a \in K$ fixed).

Hence, it makes sense to form the modified monic polynomial

$$F_a(X) = \prod_{\overline{g} \in G/G_a} (X - g(a)) \in K[X]$$

and the preceding calculations show that by varying across $\overline{g} \in G/G_a$ the values $g(a) \in K$ involve *no repetitions*. Thus, F_a is a *separable* polynomial over K. Obviously $F_a(a) = 0$, so if we can show that $F_a \in (K^G)[X]$ then m_a divides F_a in $(K^G)[X]$, so m_a inherits separability from F_a. In other words, we could conclude that all $a \in K$ are separable over K^G, so the normal algebraic extension K/K^G would also be separable.

To see that F_a has its coefficients in K^G, we observe that its coefficients are (up to sign) literally the elementary symmetric functions along the G-orbit of a where we now use those elements of the orbit (rather than elements of G, as in Step 1) for the indexing set of the construction of the elementary symmetric functions. In other words, the same reasoning as in Step 1 for G-invariance applies, with the only difference that now we're working with a list of elements of K involving no repetition. Overall, we have shown that K is a separable normal algebraic extension of K^G. But we haven't yet proved it is of finite degree!

Step 3: Now we prove that $[K : K^G]$ is finite, and more specifically that $[K : K^G] \leq \#G$. For this purpose we use the Primitive Element Theorem in a novel way. Consider an arbitrary subextension $F \subset K$ over K^G with *finite* degree over K^G. (For example, if $a_1, \ldots, a_n \in K$ is a finite set of elements, all of which we know are algebraic over K^G, then we could take F to be $K^G(a_1, \ldots, a_n)$.) I claim that $[F : K^G] \leq \#G$ regardless of the choice of F. This *uniform* upper bound independent of F will then be used to deduce that in fact K itself is of finite degree over K^G, with degree at most $\#G$.

By the known separability of K over K^G, the *finite* subextension F/K^G is separable. Hence, by the Primitive Element Theorem, $F = K^G(a)$ for some $a \in F$. But then $[F : K^G] = \deg m_a \leq \deg F_a = [G : G_a] \leq \#G$. Voila, the desired uniform upper bound is established. Since there is such an upper bound that is independent of F, there must be a maximal value for $[F : K^G]$ (at most $\#G$) as we vary across all such F. So pick an $E \subset K$ of finite degree over K^G for which $[E : K^G]$

is as big as possible. I claim that necessarily $E = K$, so we will have established that $[K : K^G]$ is finite and at most $\#G$.

Pick any $b \in K$. We want to show that $b \in E$. Certainly $E(b)$ is a finite extension of E since b is even algebraic over $K^G \subset E$, so $E(b)$ is finite over K^G (as E is finite over K^G, and finiteness of degree is transitive in towers of field extensions). Thus, $[E(b) : K^G] \leq [E : K^G]$ by the optimizing way in which E was chosen. But by multiplicativity of field degree,

$$[E(b) : K^G] = [E(b) : E][E : K^G] \geq [E : K^G].$$

This forces $[E(b) : K^G] = [E : K^G]$, so $[E(b) : E] = 1$, which is to say $b \in E$ as desired.

Step 4: Now K is known to be a finite Galois extension of K^G with $[K : K^G] \leq \#G$. But recall that by the definitions, we have $G \subset \mathrm{Aut}(K/K^G) = \mathrm{Gal}(K/K^G)$, so $\#G \leq \#\mathrm{Gal}(K/K^G)$. However, as for any finite Galois extension, $\#\mathrm{Gal}(K/K^G) = [K : K^G]$. We have shown that $[K : K^G] \leq \#G$, so the opposing inequalities must be equalities. In other words, necessarily $\#G = [K : K^G] = \#\mathrm{Gal}(K/K^G)$. Thus, the inclusion $G \subset \mathrm{Gal}(K/K^G)$ of finite groups must be an equality due to size reasons. This completes the proof of Artin's Lemma.

2. Fundamental Theorem and consequences

With Artin's Lemma established, we will get lots of nice consequences right away. Let K/k be a finite Galois extension with Galois group G, and let H be any subgroup of G. Consider the fixed field $K^H \subset K$ over k. This is a finite Galois extension, since K is Galois over every subfield over k (why?). Since $k \subset K^H$, certainly $\mathrm{Gal}(K/K^H) \subset \mathrm{Gal}(K/k) = G$, and this subgroup of G contains H (why?). I claim that the containment

$$H \subset \mathrm{Gal}(K/K^H)$$

is always an equality (i.e., if we begin with a subgroup H of G, form the associated fixed field, and then form the subgroup of G associated to that fixed field, we get back H and not something bigger). Indeed, Artin's Lemma tells us that K/K^H is a finite Galois extension (which we already knew) and that the natural inclusion $H \subset \mathrm{Aut}(K/K^H)$ (which is exactly what is being considered!) is an equality. Voila.

And we also get the reserve version of the correspondence: for a subfield $F \subset K$ over k (over which K is necessarily Galois – why?) and the corresponding subgroup $H := \mathrm{Aut}(K/F) = \mathrm{Gal}(K/F) \subset \mathrm{Gal}(K/k) = G$ of elements of G that pointwise fix F, the natural inclusion $F \subset K^H$ (why does this hold?) is in fact an equality. This is just a matter of comparing degrees: by multiplicativity

$$[K : F] = [K : K^H][K^H : F]$$

yet $[K : F] = \#\mathrm{Gal}(K/F) = \#H$ and Artin's Lemma gives $[K : K^H] = \#H$ too, so $[K^H : F] = 1$; i.e., the containment $F \subset K^H$ inside K is an equality. This completes the proof that the two operations in the Galois correspondence are indeed reverse to each other.

Let's record some additional useful features of the Galois correspondence, going beyond comparison of equalities between subextensions and subgroups:

Proposition 2.1. *Let K/k be a finite Galois extension with Galois group G. Let $F, F' \subset K$ be subfields over k, and $H = \mathrm{Gal}(K/F)$, $H' = \mathrm{Gal}(K/F')$ the corresponding subgroups of G. Then $F \subset F'$ inside K if and only if $H' \subset H$ inside G.*

Moreover, $F \cap F'$ corresponds to the subgroup HH' of G generated by H and H', and the compositum FF' over k corresponds to the subgroup $H \cap H'$ of G.

Beware that if neither H nor H' is normal in G then HH' need not consist solely of elements of the form hh' (or $h'h$) for $h \in H$ and $h' \in H'$.

Proof. If $F \subset F'$ then any k-automorphism of K fixing F' pointwise certainly fixes F pointwise, which is to say $H' \subset H$. Conversely, if this inclusion of groups holds then any element of K fixed by all elements of H is certainly fixed by all elements of H'. This says $K^H \subset K^{H'}$, but $K^H = F$ and $K^{H'} = F'$, so $F \subset F'$.

Now that we have translated field and group inclusions across both sides of the Galois correspondence, noting that it reverses inclusions in each direction, we see that the biggest subfield $F \cap F'$ of K over k contained in both F and F' must correspond to the smallest subgroup of G containing both H and H'. This smallest subgroup is nothing other than HH'. Likewise, the smallest subfield FF' of K over k containing both F and F' corresponds to the biggest subgroup of G contained in both H and H'; i.e., FF' corresponds to $H \cap H'$. ■

Proposition 2.2. *Let K/k be a finite Galois extension with Galois group G. For any subfield $F \subset K$ over k and its associated subgroup $H = \mathrm{Gal}(K/F)$, $[F : k] = [G : H]$.*

Also, for any $g \in G$, the subgroup associated to the subextension $g(F) \subset K$ over k is gHg^{-1}, and F/k is Galois (equivalently, normal) if and only if H is normal in G. In such cases, the natural restriction map

$$G = \mathrm{Aut}(K/k) \to \mathrm{Aut}(F/k) = \mathrm{Gal}(F/k)$$

is surjective with kernel H, so it identifies the group G/H with $\mathrm{Gal}(F/k)$.

If H is not assumed to be normal in G then G/H makes sense as a set of cosets, and as such one can naturally identify G/H with the set $\mathrm{Hom}_k(F, K)$ of k-embeddings of F into K. This is a refinement of the equality $[G : H] = [F : k]$, and we leave it to the interested reader to think about this assertion (which we will not need).

Proof. By multiplicativity of field degrees,

$$[F : k] = [K : k]/[K : F] = \#G/\#H = [G : H].$$

For any $g \in G$, the subgroup of G associated to $g(F)$ consists of those $g' \in G$ such that $g'(g(x)) = g(x)$ for all $x \in F$, and by applying g^{-1} to both sides it is equivalent to say $(g^{-1}g'g)(x) = x$ for all $x \in F$. By the Galois dictionary, this latter condition says exactly that $g^{-1}g'g \in H$, or in other words $g' \in gHg^{-1}$.

By our normality criterion, a subextension F of K/k is normal (equivalently, Galois) over k if and only if it is stable under the action of every $g \in \mathrm{Aut}(K/k) = G$, which is to say $F = g(F)$ for all $g \in G$. By the Galois dictionary, this says that the associated subgroups of G coincide, which is to say $H = gHg^{-1}$ for all $g \in G$. This latter condition expresses exactly the normality of H in G.

Finally, in our earlier study of normal extensions we showed that when a subextension F of K/k is also normal over k then the resulting restriction map on k-automorphism groups is surjective, which is to say that $G \to \mathrm{Gal}(F/k)$ is surjective. It kernel consists of exactly those $g \in G$ that act trivially on F, which is $\mathrm{Gal}(K/F) = H$ by definition. Hence. $G/H \simeq \mathrm{Gal}(F/k)$ as groups. ■

3. An example

Let L be the splitting field over $\mathbf{Q}$ of $f = X^8 - 2$ (which is irreducible by Eisenstein's criterion). Let $\alpha \in L$ be a root of f. The ratios among the 8 distinct roots of f in L are 8 distinct 8th roots of unity, so L contains a primitive 8th root of unity ζ. The subfield $\mathbf{Q}(\alpha, \zeta) \subset L$ must exhaust L since the elements $\alpha\zeta^j$ ($j \in \mathbf{Z}/8\mathbf{Z}$) exhaust the set of roots of f. Hence, $L = \mathbf{Q}(\alpha, \zeta)$. We want to explicitly compute $G = \mathrm{Gal}(L/\mathbf{Q})$.

As a first step, let's compute $[L : \mathbf{Q}]$. The subfield $\mathbf{Q}(\alpha)$ has $\mathbf{Q}$-degree $\deg(f) = 8$ (why?), and L is generated over $\mathbf{Q}(\alpha)$ by the element ζ that satisfies $\zeta^4 = -1$, so $[L : \mathbf{Q}(\alpha)] \leq 4$. By direct

calculation

$$(\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = i + 2 - i = 2,$$

yet $\pm\alpha^4$ are two square roots of 2 (!), so $\zeta + \zeta^{-1} = \pm\alpha^4 \in \mathbf{Q}(\alpha)$. More specifically, $\zeta^2 + 1 = \pm\alpha^4\zeta$, so $\zeta^2 \mp \alpha^4\zeta + 1 = 0$. This shows that ζ satisfies a quadratic polynomial over $\mathbf{Q}(\zeta)$, so $[L : \mathbf{Q}(\alpha)] \leq 2$. But this degree cannot be 1 (i.e., $L \neq \mathbf{Q}(\alpha)$) since $\mathbf{Q}(\alpha)$ admits an embedding into $\mathbf{R}$ (sending α to either of the two 8th roots of 2 in $\mathbf{R}$) yet $\mathbf{R}$ does not contain a primitive 8th root of unity. Hence, $[L : \mathbf{Q}(\alpha)] = 2$, so $[L : \mathbf{Q}] = [L : \mathbf{Q}(\alpha)][\mathbf{Q}(\alpha) : \mathbf{Q}] = 2 \cdot 8 = 16$.

Since $\pm i = \zeta^2$ likewise lies in L yet not in $\mathbf{Q}(\alpha)$, even $\mathbf{Q}(\alpha, i)$ has to exhaust L by $\mathbf{Q}(\alpha)$-degree reasons. That is, $L = \mathbf{Q}(\alpha, i)$. This can also be seen quite explicitly: we saw above that $\zeta^2 \mp \alpha^4\zeta + 1 = 0$, yet $\zeta^2 = \pm i$, so if we *define* $i = \zeta^2 \in L$ to remove sign ambiguity then $\pm\alpha^4\zeta = 1 + i$, so $\zeta = \pm(1 + i)/\alpha^4$. This explicitly exhibits ζ inside $\mathbf{Q}(\alpha, i) = L$.

From our determination of the $\mathbf{Q}$-degree we see that the finite group $G = \mathrm{Gal}(L/\mathbf{Q})$ has size 16, and for any $g \in G$ the effects on the generators α and i of $L = \mathbf{Q}(\alpha, i)$ over $\mathbf{Q}$ must be given by $g(\alpha) = \zeta^j\alpha$ for some $0 \leq j \leq 7$ and $g(i) = \pm i$ (why?). This gives at most 16 possibilities for g, yet we know that $\#G = 16$, so all 16 possibilities *do* occur! (Note here that it was important for us to recognize that $L = \mathbf{Q}(\alpha, i)$ rather than merely $L = \mathbf{Q}(\alpha, \zeta)$, to cut down on the list of possibilities for descriptions of $g \in G$. Otherwise we effectively would have had to make use of the algebraic relation $\zeta^2 \mp \alpha^4\zeta + 1 = 0$ to rediscover the required constraints to whittle down a list of 32 possible automorphisms to a list of 16, expressed in terms of α and ζ rather than in terms of α and i.)

Consider the automorphisms $\sigma, \tau \in G$ characterized by the conditions

$$\sigma(\alpha) = \zeta\alpha, \sigma(i) = i, \quad \tau(\alpha) = \alpha, \tau(i) = -i.$$

(We know that such automorphisms *really exist* precisely because we enumerated a list of the only 16 possible automorphisms and deduced from the knowledge of $\#G$ that these do all occur.) By direct calculation, we see that $\tau^2 = 1$ (so τ has order exactly 2, as it is certainly not trivial). The story for σ requires some more thought since we need to express ζ in terms of α and $i = \zeta^2$ to compute powers of σ (all of which fix i). Since $\zeta = \pm(i+1)/\alpha^4$, we have $\sigma(\zeta) = \pm(i+1)/(\zeta\alpha)^4 = \mp(i+1)/\alpha^4 = -\zeta$ since $\zeta^4 = -1$. Thus,

$$\sigma^2(\alpha) = \sigma(\zeta\alpha) = -\zeta^2\alpha = -i\alpha, \;\; \sigma^3(\alpha) = -i(\zeta\alpha) = -\zeta^3\alpha, \;\; \sigma^4(\alpha) = \zeta^3(\zeta\alpha) = -\alpha,$$

so σ^8 fixes α and i; i.e., $\sigma^8 = 1$ but $\sigma^4 \neq 1$ (it negates α), so σ has order exactly 8. This calculation also shows that $\sigma^j(\alpha) = \pm\zeta^j\alpha$, where the sign depends on j in a way that we won't need to make precise.

We conclude that $\langle\sigma\rangle$ has index 2 in G whereas $\langle\tau\rangle$ has index 8 in G, so the corresponding fixed fields L^σ and L^τ have respective $\mathbf{Q}$-degrees 2 and 8. This forces the evident (!) inclusions $\mathbf{Q}(i) \subset L^\sigma$ and $\mathbf{Q}(\alpha) \subset L^\tau$ to be equalities.

Let's now figure out the description of G. Since $\mathbf{Q}(i)$ is Galois over $\mathbf{Q}$, the corresponding subgroup $\langle\sigma\rangle$ is normal in G (though this is obvious directly, since index-2 subgroups are always normal). Hence, τ-conjugation preserves $\langle\sigma\rangle$, so $\tau\sigma\tau^{-1} = \sigma^j$ for some $j \in \mathbf{Z}/8\mathbf{Z}$. What is j? We can figure this out by computing the effect on α since $\langle\sigma\rangle = \mathrm{Gal}(L/\mathbf{Q}(i))$ with $L = (\mathbf{Q}(i))(\alpha)$. More specifically,

$$(\tau\sigma\tau^{-1})(\alpha) = \tau(\sigma(\alpha)) = \tau(\zeta\alpha) = \tau(\zeta)\alpha.$$

What is $\tau(\zeta)$ (as a power of ζ)? This can be seen in a couple of ways. Firstly, we saw that $\zeta = \pm(i+1)/\alpha^4$, so $\tau(\zeta) = \pm(-i+1)/\alpha^4$ is complex conjugation when L is put into $\mathbf{C}$ via sending α to an 8th root of 2 in $\mathbf{R}$; hence, $\tau(\zeta) = \zeta^{-1}$ (since complex conjugation acts as inversion on *all* roots of unity in $\mathbf{C}$; why?). One can see the same reasoning from the description of L as $\mathbf{Q}(\alpha, i)$ via the characterization of τ in its effects on α and i (without special focus on how ζ sits inside L).

Anyway, continuing our calculation,

$$(\tau\sigma\tau^{-1})(\alpha) = \tau(\zeta)\alpha = \zeta^{-1}\alpha = \sigma^{-1}(\alpha)$$

(check the final equality). Thus,

$$\tau\sigma\tau^{-1} = \sigma^{-1}.$$

The group G with order 16 has generators σ and τ with respective orders 8 and 2 such that the normal subgroup of order 8 generated by σ is acted upon through inversion under τ-conjugation. This shows that the generators σ and τ satisfy the relations that give a presentation of the dihedral group D_8 of order 16, so we get a surjective homomorphism $D_8 \twoheadrightarrow G$ that must be an isomorphism for size reasons.

Remark 3.1. There are plenty of other subgroups of $D_8 = G$. For example, there are the conjugates of the order-2 subgroups $\langle\tau\rangle$ by powers of σ. Explicitly, since $\tau\sigma = \sigma^{-1}\tau$, we see that $\sigma\tau = \tau\sigma^{-1}$, so $\sigma\tau\sigma^{-1} = \tau\sigma^{-2}$. Iterating, $\sigma^j\tau\sigma^{-j} = \tau\sigma^{-2j} = \sigma^{2j}\tau$, so we get 4 distinct subgroups $\langle\sigma^{2j}\tau\rangle$ of order 2 with $j = 0, 1, 2, 3$, and the corresponding fixed fields must be the G-orbit of $\mathbf{Q}(\alpha) = L^\tau$. To be explicit, $L^{\sigma^{2j}\tau} = \mathbf{Q}(\zeta^j\alpha)$ since $\sigma^j(\alpha) = \pm\zeta^j\alpha$. In other words, we have the subfield $\mathbf{Q}(i)$ Galois over $\mathbf{Q}$, and the 4 subfields $\mathbf{Q}(\alpha)$, $\mathbf{Q}(\zeta\alpha)$, $\mathbf{Q}(\zeta^2\alpha) = \mathbf{Q}(i\alpha)$, and $\mathbf{Q}(\zeta^3\alpha)$ of degree 8 over $\mathbf{Q}$.

There are yet more subfields. For example, the presentation of D_8 shows that it maps onto $\mathbf{Z}/(2) \times \mathbf{Z}/(2)$ via sending σ onto $(1, 0)$ and τ onto $(0, 1)$ (this is the abelianization of D_8), so this provides three order-2 quotients of $G = D_8$ that must correspond to *three* subfields of L which are quadratic over $\mathbf{Q}$. But we know these subfields: they're the ones in the subfield $\mathbf{Q}(\zeta)$ whose Galois group over $\mathbf{Q}$ is $(\mathbf{Z}/8\mathbf{Z})^\times$ and hence must be the abelization of D_8 (for size reasons). In the final 2 pages of §14.2 the full lattice of subgroups and corresponding subfields is worked out in detail.