M3P11 (and M4P11, M5P11) Galois Theory, Worksheet 3v2

Alessio Corti

9th February 2020*

Q 1. Prove that $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{-3}, \sqrt[3]{5})$ is a normal extension. What is its degree?

Q 2. Establish (with proofs) whether the following extensions of $\mathbb{Q}$ are normal or not:

(i) $\mathbb{Q}(\sqrt{6})$;

(ii) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$;

(iii) $\mathbb{Q}(7^{1/3})$;

(iv) $\mathbb{Q}(7^{1/3}, e^{2\pi i/3})$;

(v) $\mathbb{Q}(\sqrt{1+\sqrt{7}})$;

(vi) $\mathbb{Q}(\sqrt{2+\sqrt{2}})$.

Q 3. (a) Prove that if $E \subset F$ and $[F : E] = 2$ then the extension is normal.
(b) Prove that every index 2 subgroup of a group G is normal.

Q 4. Say $E = \mathbb{Q}$ and let F be the splitting field of $x^p - 1$, where p is an odd prime number.
(i) What is $[F : E]$? What is $\mathrm{Gal}(F/E)$?

(ii) Prove that there is a unique subfield K of F with $[K : \mathbb{Q}] = 2$ [*Hint: Part (i), plus the fact that* $(\mathbb{Z}/p\mathbb{Z})^\times$ *is cyclic*]. Show that all such extensions are of the form $K = \mathbb{Q}(\sqrt{n})$ where $n \in \mathbb{Z}$ and $|n|$ is squarefree.[1] Figure out n when $p = 3$. Figure out n when $p = 5$ [*Hint: what is* $\cos(2\pi \boldsymbol{i}/5)$*?*]. What do you think the answer is in general? (This is a number-theoretic question rather than a field-theoretic one so don't get frustrated if you see a good-looking statement but you can't prove it: there are tricks but they're tough to spot even for me.)

Q 5. (i) Say $a, b > 1$ are distinct squarefree integers. Prove $x^2 - a$ is irreducible, so $\mathbb{Q}(\sqrt{a})$ has degree 2 over $\mathbb{Q}$. Now prove that $\sqrt{b} \notin \mathbb{Q}(\sqrt{a})$.

(ii) Let F be the splitting field of $(x^2 - a)(x^2 - b)$ over $\mathbb{Q}$. What is $\mathrm{Gal}(F/\mathbb{Q})$? Use the fundamental theorem of Galois theory to find all the fields K with $\mathbb{Q} \subseteq K \subseteq F$. Which ones are normal over $\mathbb{Q}$?

*v2 28th April 2020

[1] A natural number is squarefree if it is the product of distinct primes.

(iii) Prove that $F = \mathbb{Q}(\sqrt{a}+\sqrt{b})$. [*Hint: figure out which subgroup of the Galois group this field corresponds to.*]

(iv) Let p, q and r be distinct primes. Prove $\sqrt{r} \notin \mathbb{Q}(\sqrt{p}, \sqrt{q})$. [*Hint: use one of the previous parts.*]

(v) Conclude that if $F = \mathbb{Q}(\sqrt{p}, \sqrt{q}, \sqrt{r})$ then $[F : \mathbb{Q}] = 8$. What is $\mathrm{Gal}(F/\mathbb{Q})$?

(vi) Use the fundamental theorem of Galois theory to write down all the intermediate subfields between $\mathbb{Q}$ and F. If you can't then just write down the subfields E of F with $[E : \mathbb{Q}] = 2$.

(vii) Show that (notation as in the previous part) $F = \mathbb{Q}(\sqrt{p}+\sqrt{q}+\sqrt{r})$.

(viii) Prove that if $p_1, p_2, \ldots, p_n$ are distinct primes, then $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n})$ has degree 2^n over $\mathbb{Q}$, and equals $\mathbb{Q}(\sqrt{p_1}+\sqrt{p_2}+\cdots+\sqrt{p_n})$.

Q 6. Say $r = \sqrt[11]{5^{1/3}+\sqrt{8^{1/5}+6}} + 9^{1/7}$. Find a sequence of fields $\mathbb{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n$ with $r \in F_n$ and such that for all i we have $F_i = F_{i-1}(\alpha_i)$ with $\alpha_i^{n_i} \in F_{i-1}$ for some positive integer n_i.

Q 7. Fix a normal and separable extension of fields $K \subset L$ and let G be the Galois group. Recall the standard notation of the Galois correspondence: for $K \subset F \subset L$, $F^\dagger \subset G$ is the group that fixes F; for $H \leq G$, $H^\star$ is the fixed field of H.[2]

(a) Let $K \subset F$ be an intermediate field. Let $X = \mathrm{Emb}_K(F, L)$.[3] Observe that composition of functions gives a natural (left) action of G on X. Show that this action is *transitive*, that is, for all $x, y \in X$ there is $g \in G$ with $gx = y$. Why does this generalise the statement about the transitive action of G on the roots of a polynomial? For x in X denote by G the stabiliser of x:

$$G_x = \{x \in G \mid gx = x\}$$

Prove that $G_x = x^\dagger$, i.e., the group that fixes F where F is viewed as an intermediate field via the K-inclusion $x\colon F \to L$.

(b) Let $K \subset F \subset L$ be an intermediate field and $H = F^\dagger$ the corresponding subgroup, i.e., $H \leq G$ is the subgroup that fixes F and $F = H^\star$ is the fixed field of H. Show that $K \subset F$ is normal if and only if $H \leq G$ is a normal subgroup. Show that in this case $K \subset F$ is separable (obvious) and $\mathrm{Emb}_K(F, F) = H\backslash G$.

(c) More generally show that for all $K \subset F \subset G$ and $H = F^\dagger$:

$$\mathrm{Emb}_K(F, F) = H\backslash N_G(H)$$

where $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ is the *normaliser* of H in G.[4] (By construction $H \leq N(H)$ is a normal subgroup and we are allowed to form the quotient group $H\backslash N(H)$.)

(d) Here and below, for $H_1, H_2 \leq G$, write

$$N(H_1, H_2) = \{g \in G \mid gH_1g^{-1} \supset H_2\}$$

[2]This is a substantially revised version of the original question.

[3]Feel free to assume that X is nonempty.

[4]Those of you who are taking *Algebraic Topology* should compare this statement with a similar statement in the theory of covering spaces.

(I don't know what this thing is called in Algebra.) Show that the assignment

$$g, h_1, g \mapsto gh_1$$

defines a *right* action $N(H_1, H_2) \times H_1 \to N(H_1, H_2)$. Here and below, denote by

$$\mathrm{Mor}(H_2, H_1) = N(H_1, H_2)/H_1$$

the quotient *set*.

Now suppose given *two* intermediate fields, $K \subset F_1 \subset L$ and $K \subset F_2 \subset L$. As usual for clarity denote by $x_1 \colon F_1 \to L$ and $x_2 \colon F_2 \to L$ the two inclusions, and let $H_1 = x_1^\dagger$, $H_2 = x_2^\dagger$. Prove that

$$\mathrm{Emb}_K(F_1, F_2) = \mathrm{Mor}(H_1, H_2)$$

(e) In this Part, G is a group and H_1, H_2, etc. are subgroups of G. Show that the function:[5]

$$T \colon N(H_1, H_2) \to \mathrm{Fun}(H_2, H_1)$$

where $N(H_1, H_2)$ is as in Part (d) and $T \colon g \mapsto T_g$, the function such that

$$T_g(h) = g^{-1}hg,$$

in fact lands in the set $\mathrm{Hom}(H_2, H_1)$ of *group homomorphisms* from H_2 to H_1.

Note that the set $N(H_1, H_2)$ is in general not a group, but that there is a natural composition law:

$$N(H_1, H_2) \times N(H_2, H_3) \to N(H_1, H_3)$$

Recall that the *centraliser* of $H \leq G$ is the subgroup

$$C(H) = \{g \in G \mid \text{for all } h \in H, hg = gh\}$$

show that $g, z \mapsto gz$ defines a left action $C(H_2) \times N(H_1, H_2) \to N(H_1, H_2)$ of $C(H_1)$ on $N(H_1, H_2)$, and that for all $g_1, g_2 \in N(H_1, H_2)$, $T_{g_1} = T_{g_2}$ if and only if there exists $z \in C(H_2)$ such that $g_2 = zg_1$.

(f †) As in Part (b), for subgroups H_1, H_2 of G write:

$$\mathrm{Mor}(H_1, H_2) = N(H_2, H_1)/H_2$$

the quotient *set*. Show that there is a natural composition $\mathrm{Mor}(H_1, H_2) \times \mathrm{Mor}(H_2, H_3) \to \mathrm{Mor}(H_1, H_3)$ that makes the set of subgroups of G into a category.

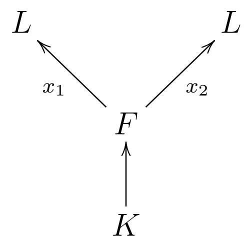
(g †) Show that the Galois correspondence is a *contravariant* equivalence of categories, from the category whose objects are intermediate fields $K \subset F \subset L$, and where the set of morphisms from F_1 to F_2 is $\mathrm{Emb}_K(F_1, F_2)$, to the category of subgroups defined in Part (e). In other words we have identifications

$$\mathrm{Emb}_K(F_1, F_2) = \mathrm{Mor}(H_2, H_1)$$

compatible with composition.

[5]For X_1, X_2 sets, I denote by $\mathrm{Fun}(X_1, X_2)$ the set of functions from X_1 to X_2.

Q 8. Let $K \subset F$ be a field extension and $K \subset L$ a normal field extension. Assume given *two* K-embeddings $x_1 \in \mathrm{Emb}_K(F, L)$, $x_2 \in \mathrm{Emb}_K(F, L)$:



(so I am saying that $x_i|K$ is the inclusion of K in L given at the beginning).

(a) Show that there is a K-embedding $y \colon L \to L$ such that $y \circ x_1 = x_2$.

(b) In the same situation as above, let now $F \subset E$ be a field extension. For $i = 1, 2$ denote by $\mathrm{Emb}_{x_i}(E, L)$ the set of field homomorphisms $\widetilde{x} \colon E \to L$ such that $\widetilde{x}|F = x_i$. Use part (a) to produce a bijective correspondence from $\mathrm{Emb}_{x_1}(E, L)$ to $\mathrm{Emb}_{x_2}(E, L)$. (In particular, this shows that one set is empty if and only if the other is empty.)

Q 9. Let $K \subset F \subset L$ be a tower of field extensions. As we stated in class, it is immediate from the definition that: If $K \subset L$ is normal, then $F \subset L$ is also normal.

(a) If $K = \mathbb{Q}$, $F = \mathbb{Q}(2^{1/3})$ and $L = \mathbb{Q}(2^{1/3}, \omega)$ with $\omega = e^{2\pi i/3}$, then show that $K \subset L$ is normal, but $K \subset F$ is not normal.

(b) If $K = \mathbb{Q}$, $F = \mathbb{Q}(\sqrt{2})$ and $E = \mathbb{Q}(2^{1/4})$, show that $K \subset F$ and $F \subset L$ are normal, but $K \subset L$ is not normal.

(c) Say $H \subseteq K \subseteq G$ are groups. Prove that if H is normal in G then H is normal in K. Give an example of groups with H is normal in G but K not normal in G. Now give an example with H normal in K, K normal in G, but H not normal in G. Now wonder whether this is all a coincidence or not.