GALOIS THEORY
Solutions to Worksheet 8

A 1. I did not mean for you to actually do ALL of this question, 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.

(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 done in the **next question**, 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 $gx(F) \subset x(F)$.[1]

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):

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

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

[1]Let's be careful about this. By definition $K \subset F$ is normal if and only if for all $K \subset \Omega$, and for all $x, y \in \mathrm{Emb}_K(F, \Omega)$, $x(F) \subset y(F)$. Prove that $K \subset F$ is normal if and only if for *some* given normal extension $K \subset \Omega$ such that $\mathrm{Emb}_K(F, \Omega) \neq \emptyset$, we have: for all $x, y \in \mathrm{Emb}_K(F, \Omega)$, $x(F) \subset y(F)$.

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 ρ 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). Now for all $g, g' \in N(H_1,H_2)$, $\rho(g) = \rho(g')$ 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).

A 2. (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

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

as follows:

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

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

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

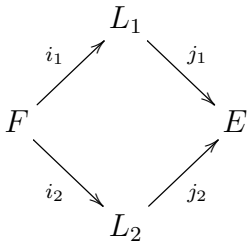
therefore, as claimed, $y_\star(\widetilde{x}) \in \mathrm{Emb}_{x_2}(E, L)$.

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

A 3. This is asking a tiny bit more than Question 5 on Worksheet 2. Go back to that question and see if you understand it better now.

A 4. (a) Fix an inclusion $L \subset \Omega$ and let $j\colon L \to \Omega$ be a K-embedding. By property (ii) in the definition of normal closure, as σ varies in $\mathrm{Emb}_K(L, L)$ the $\sigma(F)$ generate L; it follows that the $j\sigma(F)$ generate $j(L)$; but by property (i) all $j\sigma(F)$ are contained in L, hence the field that they generate, namely $j(L)$, is also contained in L; that is $j(L) \subset L$ and this shows that $K \subset L$ is a normal extension.

(b) By Axiom 4 we can construct a diagram:



where $j_1 i_1 = j_2 i_2$. All we need to show is that $j_1(L_1) = j_2(L_2)$. In fact all we need to show is that $j_1(L_1) \subset j_2(L_2)$, as the other inclusion follows from the same argument.

By property (ii) (for $F \subset L_1$), L_1 is generated by the union of the $\sigma(F)$ over $\sigma \in \mathrm{Emb}_K(F, L_1)$; hence $j_1(L_1)$ is generated by the union of the $j_1\sigma(F)$; by property (i) (for $F \subset L_2 \subset E$) these $j_1\sigma(F)$ are all contained in $j_2(L_2)$, hence the field that they generate $j_1(L_1)$ is also contained in $j_2(L_2)$.

(c) I just explain the idea, which is very simple. There are several cases to consider, corresponding to the several cases in the discussion of biquadratic extensions in the GALOIS THEORY notes. Here I just consider the case where the minimal polynomial of $\sqrt{a + \sqrt{b}}$ over K is a degree 4 polynomial, necessarily of the form

$$f(X) = X^4 - 2aX^2 + c \in K[X]$$

OK so why don't you prove the following more general statement: If $K \subset F = K(\alpha)$ is a field extension, and $f(X) \in K[X]$ is the polynomial of α, then the normal closure of $K \subset F$ is the splitting field of $f(X)$. (This statement should not be hard to show. You must go back to the two defining properties of a splitting field.)

(d) Use the more general statement that you proved in (c).

A 5. (a) It's the field of fractions of $k[T^p]$. Or, check explicitly that if $S = T^p$ then this is just the field of fractions of $k[S]$. Or check that it's a subset containing 0 and 1 and closed under $+ - \times /$.

(b) In fact any subfield of L containing k and T must contain $f(T)$ for any polynomial $f \in k[T]$ and hence it must contain $f(T)/g(T)$ if g is a non-zero polynomial. Hence $L = k(T)$ in the sense that it's the smallest subfield of L containing k and T, so $L = k(T) \subseteq K(T) \subseteq L$ and all inclusions are equalities.

(c) T is a root of the polynomial $X^p - T^p \in K[X]$.

(d) If $q(X) = X^p - T^p$ factored in $K[X]$ into two factors f and g of degrees a and b, with $a + b = p$ and $0 < a, b < p$, then by rescaling we can assume both factors are monic. Now consider the factorization $q(X) = (X - T)^p$ in $L[X]$. This is the factorization of $q(X)$ into primes in $L[X]$, and there's only one prime involved, namely $X - T$. Because $q = fg$ in $L[X]$, we must have $f(X) = (X-T)^a$ and $g(X) = (X-T)^b$ – anything else would contradict unique factorization. But this means the constant term of $f(X)$ is $\pm T^a$ and because $0 < a < p$ we know a isn't a multiple of p and hence $\pm T^a \notin K$ and so $f(X) \notin K[X]$, a contradiction.

(e) $q(X)$ is irreducible in $K[X]$ and T is a root, so it's the min poly. It's not separable because it is irreducible over K but has repeated roots in L (namely T, p times).

(f) $T \in L$ is not separable over K because its min poly isn't. Hence $K \subset L$ is not separable, because L contains an element which is not separable over K.

A 6. (a) If $F_1 = K(\alpha_1, \ldots, \alpha_n)$ then for $K \subseteq F \subseteq L$ we have that F contains F_1 iff F contains all the α_i. So if $K \subseteq F \subseteq L$ then F contains E iff F contains F_1 and F_2, iff F contains all the α_i and F_2; hence $F_2(\alpha_1, \ldots, \alpha_n)$ is the smallest subfield of L containing F_1 and F_2.

(b) If F_1 is the splitting field of $p(X) \in K[X]$ and F_2 is the splitting field of $q(X) \in K[X]$ (these polynomials exist by normality) then I claim E is the splitting field of $p(X)q(X)$; indeed if the α_i are the roots of p and β_j are the roots of q then by the first part E is the field generated by the α_i and the β_j. Now E is finite and normal; moreover each of the α_i and the β_j are separable over K (as each is contained in either F_1 or F_2) and hence each time we adjoin one we get a separable extension; finally a separable extension of a separable extension is separable (by comparing degrees and separable degrees).

(c) If $g \in G$ then $g(F_1) = F_1$ because $K \subset F_1$ is normal, and hence the restriction of g to F_1 is in G_1. Similar for $K \subset F_2$. So we get a map $G \to G_1 \times G_2$. This is easily checked to be a group homomorphism. It's injective because anything in the kernel fixes F_1 and F_2 pointwise, so fixes F_1F_2 pointwise; but $F_1F_2 = E$.

It's not always surjective though – for example if $F_1 = F_2$ then it hardly ever is. More generally if $F_1 \cap F_2 \neq K$ then there will be problems. However if $F_1 \cap F_2 = K$ then the map is a bijection.