GALOIS THEORY
Worksheet 8

Q 1. 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.

(a) Let $K \subset F$ be an intermediate field. Let $X = \mathrm{Emb}_K(F, L)$.[1] 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 $K \subset F \subset L$ 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.[2] (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

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

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

$$g, h_1 \mapsto gh_1$$

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

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

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

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

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:[3]

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

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.

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

$$\begin{tikzcd}
L & & L \\
& F \arrow[ul, "x_1"] \arrow[ur, "x_2"'] & \\
& K \arrow[u] &
\end{tikzcd}$$

(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 3. Let $K \subset L$ be a field extension, and for $i = 1, \dots, n$ let $K \subset F_i \subset L$ be intermediate fields. We say that L is *generated* by the F_i if and only if the following property holds: If $K \subset F \subset L$ and for all i $F_i \subset F$, then $F = L$.

Now let $K \subset \Omega$ be a field extension, and for $i = 1, \dots, n$ let $K \subset F_i \subset \Omega$ be intermediate fields. Show that there exists a unique field $K \subset L \subset \Omega$ generated by the F_i.

Show that the elements of $F_1 \cdots F_n$ are precisely the *finite sums* of terms of the form $a_1 \dots a_n$ where for all i $a_i \in F_i$.

Q 4 (†). Let $K \subset F$ be a field extension. In this question, we say that $F \subset L$ is a *normal closure* of $K \subset F$ if the following two conditions are satisfied:

(i) For all extensions $L \subset \Omega$ and for all K-embeddings $\sigma \colon F \to \Omega$, $\sigma(F) \subset L$;

(ii) L is generated by the images $\sigma(F)$, as $\sigma \in \mathrm{Emb}_K(F, L)$.

[**N.B.** *This is not the definition given in Video 23 of the course.*]

Prove from the definition just given that:

(a) Let $F \subset L$ be a normal closure of $K \subset F$. Prove that $K \subset L$ is a normal extension.

(b) Let $F \subset L_1$ and $F \subset L_2$ be two normal closures of $K \subset F$. Prove that there is an F-isomorphism $\sigma \colon L_1 \to L_2$.

Now answer the following:

(c) Let K be a field of characteristic $\neq 2$. For a, b in K, is it always true that the normal closure of the field extension

$$F = K\left(\sqrt{a + \sqrt{b}}\right)$$

is the field extension $L = K\left(\sqrt{a \pm \sqrt{b}}\right)$?

(d) Show that the definition given here is equivalent to the definition given in Video 23.

Q 5. Here I ask you again to go through the standard example of an inseparable extension.

Let k be any field of characteristic p (for example $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$), and let $L = k(T)$, the field of fractions of the polynomial ring $k[T]$. This means that a typical element of L is of the form $f(T)/g(T)$ with f and g polynomials, and $g \neq 0$. You can convince yourself that this is a field by checking that the sum, product etc of such things is of the same form.

Set $K = k(T^p)$, the subfield of L consisting of ratios $f(T^p)/g(T^p)$.

(a) Convince yourself that K really is a subfield of L;

(b) Check that $L = K(T)$, the smallest subfield of L containing K and T;

(c) Check that T is algebraic over K and hence $[L : K]$ is finite;

(d) Check that $q(X) = X^p - T^p$ is an irreducible element of $K[X]$.

[*Hint (i)*: suppose it were reducible, and factor it in $K[X]$. The same factorization would work in $L[X]$. But $L[X]$ is a unique factorization domain. Spot that $p(X) = (X - T)^p$ in $L[X]$. By looking at constant terms, convince yourself that this gives a contradiction. *Hint (ii)*: Eisenstein.]

(e) Deduce that $q(X)$ is the min poly of T over K, and is also an inseparable polynomial in $K[X]$;

(f) Deduce that $K \subset L$ is not a separable extension.

Q 6. Say $K \subseteq L$ is a finite field extension, and F_1 and F_2 are intermediate fields (i.e. $K \subseteq F_1 \subseteq L$ and $K \subset F_2 \subset L$). Let $E = F_1F_2 \subset L$ denote the field generated by F_1 and F_2 (as in Question 3).

(a) If $F_1 = K(\alpha_1, \ldots, \alpha_n)$ then prove $E = F_2(\alpha_1, \ldots, \alpha_n)$.

(b) Now assume $K \subset F_1$ and $K \subset F_2$ are normal. Prove $K \subset E$ is normal.

[*Hint*: splitting field.]

(c) Next assume $K \subset F_1$ and $K \subset F_2$ are normal and separable. Prove that $K \subset E$ normal and separable.

(d) Denote by G_1, G_2 and G the Galois groups of $K \subset F_1$, $K \subset F_2$ and $K \subset E$. Prove that restriction of functions gives a natural injective group homomorphism from G to $G_1 \times G_2$. Is it always surjective?