Solutions of exercise sheet 5

1. Let L/K be a finite Galois extension with Galois group G. Fix an algebraic closure $\bar{K}$ of K containing L and consider an intermediate extension $L/E/K$.

1. Prove that composition of field homomorphisms induces an action of G on the set of K-embeddings $E \longrightarrow \bar{K}$.
2. Let τ_0 be the inclusion $E \hookrightarrow \bar{K}$, and take $H = \mathrm{Stab}_G(\tau_0)$. Prove that $H = \mathrm{Gal}(L/E)$ and deduce that $L^H = E$.
3. Now assume that L is the splitting field of an irreducible separable polynomial $P \in K[X]$, and that $E = K(x_0)$ for some root x_0 of P. Show that the set of K-embeddings $E \longrightarrow \bar{K}$ is isomorphic as a G-set to the set Z_P of roots of P with the usual action of G.

Solution:

1. First, notice that each K-embedding $\tau : E \longrightarrow \bar{K}$ factors uniquely through the inclusion $i : L \hookrightarrow \bar{K}$. This just amounts to checking that L contains the image of any K-embedding $\tau : E \longrightarrow \bar{K}$. For $x \in E \subseteq L$, we easily see that $\tau(x)$ is also a root of the minimal polynomial f of x over K, because $f(\tau(x)) = \tau(f(x)) = 0$ since τ fixes all the coefficients of f. Then $\tau(x) \in L$ by normality of L, proving that τ factors through i.
   If $\tau : E \longrightarrow \bar{K}$ is a K-embedding, denote by τ^+ the unique K-embedding $E \longrightarrow L$ such that $i \circ \tau^+ = \tau$. By construction, we have $(i \circ \psi)^+ = \psi$ for each K-embedding $\psi : E \longrightarrow L$. Now we define the action of $G = \mathrm{Gal}(L/K)$ on the set of K-embeddings $E \longrightarrow \bar{K}$ via $\sigma \cdot \tau = i \circ \sigma \circ \tau^+$. Indeed, for each $\sigma_1, \sigma_2 \in G$ and each K-embedding $\tau : E \longrightarrow \bar{K}$ we have:
$$\begin{aligned}(\sigma_1\sigma_2) \cdot \tau = i \circ (\sigma_1 \circ \sigma_2) \circ \tau^+ &= i \circ \sigma_1 \circ (\sigma_2 \circ \tau^+) = i \circ \sigma_1 \circ (i \circ \sigma_2 \circ \tau^+)^+ \\ &= \sigma_1 \cdot (\sigma_2 \cdot \tau), \text{ and} \\ \mathrm{id}_L \cdot \tau = i \circ \tau^+ = \tau, &\end{aligned}$$
   so that this is an action of G on the set of K-embeddings $E \longrightarrow \bar{K}$.
2. By definition of the Galois action we gave, for $\sigma \in G$ we have that σ lies in $\mathrm{Stab}_G(\tau_0)$ if and only if
$$i \circ \sigma \circ \tau_0^+ = \tau_0.$$
   Since the right hand side can be written as $i \circ \tau_0^+$ as remarked above and i is injective, we have that the last condition is equivalent to $\sigma \circ \tau_0^+ = \tau_0^+$. But τ_0^+ is just the inclusion $E \hookrightarrow L$, so that σ lies in $\mathrm{Stab}_G(\tau_0)$ if and only if it fixes all the elements of E. This proves that $\mathrm{Stab}_G(\tau_0) = \mathrm{Gal}(L/E)$. Then by Galois correspondence we get $L^{\mathrm{Stab}_G(\tau_0)} = E$.

Please turn over!

3. Let $\mathrm{Emb}_K(E, \bar{K})$ the set of K-embeddings $E \longrightarrow \bar{K}$. For $E = K(x_0)$, such an embedding is uniquely determined by the image of x_0, which has to be a root of $P = \mathrm{Irr}(x_0; K)$. For $y \in Z_P$, let τ_y the K-embedding $E \longrightarrow \bar{K}$ sending $x_0 \mapsto y$. This defines a bijection $Z_P \longrightarrow \mathrm{Emb}_K(E, \bar{K})$ sending $y \mapsto \tau_y$. To conclude, we need to prove that this is a map of G-sets, i.e., that for each $y \in Z_P$ and $\sigma \in G$ one has $\tau_{\sigma(y)} = \sigma \cdot \tau_y$, which is equivalent to $\tau^+_{\sigma(y)} = \sigma \circ \tau^+_y$. Since the two sides consist of K-linear field homomorphisms $E = K(x_0) \longrightarrow L$, it is enough to check their equality on x_0, which is straightforward:
$$(\sigma \circ \tau^+_y)(x_0) = \sigma(y) = \tau^+_{\sigma(y)}(x_0).$$

2. (*) Let L/K be a finite Galois extension of degree n with Galois group G. For $x \in L$, let m_x be the K-linear map $L \longrightarrow L$ sending $y \mapsto xy$. We define the trace and the norm maps $\mathrm{Tr}_{L/K}, \mathrm{N}_{L/K} : L \longrightarrow K$ as
$$\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}(m_x) \quad \text{and} \quad \mathrm{N}_{L/K}(x) = \det(m_x).$$

[See Exercise sheet 11 from Algebra I, HS14]

1. Let $x \in L$. Denote $\chi_x(X) \in K[X]$ the characteristic polynomial of m_x, and $d_x = [K(x) : K]$. Prove: $\chi_x = (\mathrm{Irr}(x; K))^{n/d}$.
2. Show that for each $x \in L$ we have
$$\mathrm{Tr}_{L/K}(x) = \sum_{\sigma \in G} \sigma(x) \quad \text{and} \quad \mathrm{N}_{L/K}(x) = \prod_{\sigma \in G} \sigma(x).$$
3. Show that if $M/L/K$ is a tower of Galois extensions, then $\mathrm{N}_{M/K} = \mathrm{N}_{L/K} \circ \mathrm{N}_{M/L}$.

Notice that the last property in fact holds for any tower of finite extension, but the proof is more complicated.

Solution:

1. Let $m = n/d$. We have $K(x) = \bigoplus_{j=0}^{d-1} Kx^j$, and we can fix a $K(x)$-basis $\{\beta_1, \ldots, \beta_m\}$ of L, so that L has K basis $\{x^j\beta_i\}_{\substack{i=1,\ldots,m \\ j=0,\ldots,d-1}}$ with lexicographical order
$$\beta_1, x\beta_1, x^2\beta_1, \ldots, x^{d-1}\beta_1, \beta_2, x\beta_2, \ldots, x^{d-1}\beta_2, \ldots, \beta_m, \ldots, x^{d-1}\beta_m.$$
Let $[c_{ij}]_{0 \le i,j \le d}$ be $[m_x]_{K(x)/K}$, the $d \times d$ matrix of the K-linear map $y \mapsto xy$ of $K(x)$, so that for $j = 0, \ldots, d-1$ we have $x \cdot x_j = \sum_{i=0}^{d-1} c_{ij} x^i$. Then $\chi_{K(x)/K,x}$ be the characteristic polynomial of $[c_{ij}]$. Then by the Hamilton-Cayley theorem $\chi_{K(x)/K,x}(m_x)$ is the zero endomorphism of $K(x)$. Since $m_x^l = m_{x^l}$ and m_{x^l} is K-linear for each non-negative integer l, we easily see that $m_{\chi_{K(x)/K,x}(x)}$ is the zero endomorphism of $K(x)$, which means that $\chi_{K(x)/K,x}(x) = 0$. Since $\chi_{K(x)/K,x}(X)$ is a monic degree-d polynomial with root x, we necessarily have $\chi_{K(x)/K,x} = \mathrm{Irr}(x; K)$, and we are only left to prove that $\chi_x = \chi^m_{K(x)/K,x}$.

See next page!

To prove this last equality, we use the K-basis $\{x^j\beta_i\}$ of L and notice that $x\cdot x_j\beta_i = \sum_{\lambda=0}^{d-1} c_{\lambda j}x^\lambda\beta_i = \sum_{\lambda=0}^{d-1}\sum_{\mu=1}^{m} c_{\lambda j}\delta_{\mu,i}x^\lambda\beta_i$. Then the matrix of m_x seen as a K-endomorphism of L, with respect to the chosen basis, consists of $d\times d$ blocks, which are non-zero only when they are diagonal blocks, in which case they coincide with $[c_{ij}]$. This proves that $\chi_x = \chi_{K(x)/K,x}^m$ as desired.

2. We have that $\prod_{\sigma\in G}(X-\sigma(x))$ lies in $L^G[X]=K[X]$ and has x as a root. Notice that this polynomial may have multiple roots. More precisely, $\sigma(x)=\tau(x)$ if and only if $\sigma H = \tau H$, where $H=\{\sigma\in G : \sigma(x)=x\} = \mathrm{Gal}(L/K(x))$. In particular, $|H| = [L:K(x)] = n/d = m$, so that by choosing a set of d representatives σH for G/H, we get

$$\begin{aligned}\prod_{\sigma\in G}(X-\sigma(x)) &= \prod_{\sigma H\in G/H}\prod_{\tau\in H}(X-\sigma\tau(x)) = \prod_{\sigma H\in G/H}(X-\sigma(x))^m \\ &= \left(\prod_{\sigma H\in G/H}(X-\sigma(x))\right)^m.\end{aligned}$$

The polynomial $\prod_{\sigma H\in G/H}(X-\sigma(x))$ is also invariant under G, so that it lies in $K[X]$. Since it is monic and it has degree $d=[K(x):K]$, it must coincide with $\mathrm{Irr}(x;K)$. Then by previous point we obtain $\chi_x = \prod_{\sigma\in G}(X-\sigma(x))$, and by comparing the coefficients of degree $n-1$ and 0 we get

$$-\mathrm{Tr}_{L/K}(x) = -\sum_{\sigma\in G}\sigma(x) \quad\text{and}\quad (-1)^n\mathrm{N}_{L/K}(x) = (-1)^n\prod_{\sigma\in G}\sigma(x),$$

since the coefficients of degree $n-1$ and 0 of χ_x are, respectively, $-\mathrm{Tr}(m_x)$ and $(-1)^n\det(m_x)$. By simplifying a sign, we get the desired descriptions of the trace and the norm.

3. Let $P=\mathrm{Gal}(M/K)$. Then by the Galois correspondence $P/H\cong G$, where $H = \mathrm{Gal}(M/L)$, where the isomorphism in induced by the restriction to L of the K-automorphisms of M. This will motivate the passage $(*)$ in the coming chain of equalities. For $x\in M$, by previous point we have

$$\begin{aligned}(\mathrm{N}_{L/K}\circ\mathrm{N}_{M/L})(x) &= \prod_{\tau\in G}\tau\left(\prod_{\sigma\in H}\sigma(x)\right) \overset{(*)}{=} \prod_{\tau H\in P/H}\tau|_L\left(\prod_{\sigma\in H}\sigma(x)\right) \\ &= \prod_{\tau H\in P/H}\prod_{\sigma\in H}\tau\sigma(x) = \prod_{\xi\in P}\xi(x) = \mathrm{N}_{M/K}(x),\end{aligned}$$

where the product on "$\tau H\in P/H$" takes a set of representatives of cosets of H, and we have used the fact that the cosets of H form a partition of P.

3. Let L/K be a finite Galois extension with Galois group G.

1. Prove that the action of G on $L[X]$ (as seen in class) extends to an action on the field of rational functions $L(X)$ via $\sigma\cdot\left(\frac{P}{Q}\right) = \frac{\sigma(P)}{\sigma(Q)}$.

Please turn over!

2. Check that $L(X)^G = K(X)$.

Solution:

1. We need to check that $\sigma \cdot \left(\frac{P}{Q}\right) = \frac{\sigma(P)}{\sigma(Q)}$ gives indeed a well defined map $L(X) \longrightarrow L(X)$ for each $\sigma \in G$. Suppose that $P/Q = P'/Q'$. Then $PQ' - QP' = 0$, and

$$\sigma \cdot \left(\frac{P}{Q}\right) - \sigma \cdot \left(\frac{P'}{Q'}\right) = \frac{\sigma(P)}{\sigma(Q)} - \frac{\sigma(P')}{\sigma(Q')} = \frac{\sigma(P)\sigma(Q') - \sigma(Q)\sigma(P')}{\sigma(Q)\sigma(Q')} =$$
$$= \frac{\sigma(PQ' - QP')}{\sigma(QQ')} = \frac{\sigma(0)}{\sigma(QQ')} = 0,$$

because $\sigma\cdot$ respects sums and multiplication on $L[X]$. Hence the map is well-defined. The axioms of group action for G on $L(X)$ follow immediately from the corresponding axioms for the action of G on $L[X]$.

2. It is clear that $K(X) \subseteq L(X)^G$. Conversely, assume that $P/Q \in L(X)^G$, and, without loss of generality, that P and Q are coprime polynomials in $L(X)$, with Q monic. Then for each σ we have

$$\frac{\sigma(P)}{\sigma(Q)} = \frac{P}{Q},$$

and the only possibility is that $\sigma(P) = f_\sigma \cdot P$, $\sigma(Q) = f_\sigma \cdot Q$ for some $f_\sigma \in L[X]$, because $(P, Q) = 1$. As σ does not change the degree of the polynomials on which it acts, we actually have that $f_\sigma \in L$. Moreover, σ fixes the leading coefficient of Q (which is $1 \in K$), so that the only possibility is $f_\sigma = 1$. Then $P, Q \in L[X]^G = L^G[X] = K[X]$, so that indeed $P/Q \in K(X)$.

4. For any field K, we consider the projective line

$$\mathbb{P}(K) := (K^2 \setminus \{0\})/\sim,$$

where $(a, b) \sim (c, d)$ if there exists $\lambda \in K^\times$ such that $(c, d) = (a\lambda, b\lambda)$.

1. Check that $\sim$ is indeed an equivalence relation.
2. Prove that for any field extension L/K the map $(x, y) \mapsto (x, y)$ induces an injection $j : \mathbb{P}(K) \hookrightarrow \mathbb{P}(L)$.

From now on, assume that L/K is a finite Galois extension with Galois group G.

3. Prove that $\sigma \cdot (a, b) = (\sigma(a), \sigma(b))$ gives a well-defined action of G on $\mathbb{P}(L)$.
4. Check that $\mathbb{P}(L)^G$ is the image of $\mathbb{P}(K)$ via the injection j.

Solution:

See next page!

1. Reflexivity of $\sim$ is clear (by taking $\lambda = 1$). Now suppose that $(c,d) \sim (a,b)$, with $(c,d) = (a\lambda, b\lambda)$ for some $\lambda \in K^\times$. Then $(a,b) = (a\lambda\frac{1}{\lambda}, b\lambda\frac{1}{\lambda}) = (\frac{1}{\lambda}c, \frac{1}{\lambda}d)$, so that $(a,b) \sim (c,d)$ proving symmetry (we used the fact that $\lambda \in K^\times$ is invertible).

   Now assume that $(a,b) \sim (c,d) \sim (e,f)$ with $(e,f) = (\lambda c, \lambda d)$ and $(c,d) = (\mu a, \mu b)$ for some $\lambda, \mu \in K^\times$. Then $(e,f) = (\lambda\mu a, \lambda\mu b)$, and $\lambda\mu \neq 0$, giving $(a,b) \sim (e,f)$, which proves transitivity.

2. To avoid confusion, we call $\sim_K$ (resp., $\sim_L$) the equivalence relation defined on $K^2 \backslash \{0\}$ (resp., $L^2 \backslash \{0\}$). We have clearly an inclusion $(K^2 \backslash \{0\}) \hookrightarrow (L^2 \backslash \{0\})$ (via $(x,y) \mapsto (x,y)$), which induces a well defined map $j : \mathbb{P}(K) \longrightarrow \mathbb{P}(K)$, because if $(a,b) \sim_K (c,d)$, then $(a,b) \sim_L (c,d)$ since $K^\times \subseteq L^\times$. To prove that j is injective amounts to checking that whenever $(a,b) \sim_L (c,d)$ for $(a,b),(c,d) \in (K^2 \setminus \{0\})$, then actually $(a,b) \sim_K (c,d)$. This is immediate, since $(a,b) \sim_L (c,d)$ implies that $c = \lambda a$ and $d = \lambda b$ for $\lambda \in L^\times$, and since one out of a and b is non-zero - by simplicity, suppose a - we get $\lambda = c/a \in K \cap L^\times = K^\times$.

3. Since automorphisms of L are injective, they never send a non-zero element to zero, so that G acts on $L^2 \setminus \{0\}$ via $\sigma \cdot (x,y) = (\sigma(x), \sigma(y))$. To prove that this gives an action on $\mathbb{P}(L)$, we need to check independence from $\sim_L$. Suppose that $\sigma \in G$, and that $(c,d) = (\lambda a, \lambda b) \in (L^2 \setminus \{0\})$ for some $\lambda \in L^\times$. Then

$$\sigma \cdot (c,d) = (\sigma(\lambda a), \sigma(\lambda b)) = (\sigma(\lambda)\sigma(a), \sigma(\lambda)\sigma(b)) \sim_L (\sigma(a), \sigma(b)) = \sigma \cdot (a,b),$$

   and $\sigma\cdot$ is a well-defined map $\mathbb{P}(L) \longrightarrow \mathbb{P}(L)$. The axioms of group action follow immediately from the definition.

4. An element in $j(\mathbb{P}(K))$ has a representative of the form (a,b) with $a,b \in K$ not simultaneously zero. It is clear that G acts trivially on such a representative, so that $j(\mathbb{P}(K)) \subseteq \mathbb{P}(L)^G$.

   Conversely, assume that (α, β) represents an element in $\mathbb{P}(L)$ which is fixed by any $\sigma \in G$. If $\alpha = 0$, then $\beta \in L^\times$, and multiplication by the scalar β^{-1} gives $(\alpha,\beta) = (0,\beta) \sim_L (0,1)$, which represents $j([(0,1)]_{\sim_K})$. Else $\alpha \neq 0$, and multiplication by the scalar α^{-1} gives $(\alpha,\beta) \sim_L (1, \alpha^{-1}\beta)$. Since each $\sigma \in G$ fixes this class, we have $(1, \alpha^{-1}\beta) \sim_L (1, \sigma(\alpha^{-1}\beta))$, and the only possible scalar factor is 1, so that $\alpha^{-1}\beta \in L^G = K$, and (α,β) represents a class in $\mathbb{P}(L)$ lying in the image of j.

5. Let $f \in \mathbb{Q}[X]$ be a monic polynomial of degree $n > 2$, and L_f its splitting field over $\mathbb{Q}$. Let $G_f = \mathrm{Gal}(L/K)$, and suppose that the inclusion $G_f \hookrightarrow S_n$ is an isomorphism.

1. Show that f is irreducible over $\mathbb{Q}$
2. Given a root α of f, prove that the only automorphism of the field $\mathbb{Q}(\alpha)$ is the identity.

Solution:

1. Suppose that f factors as $f = gh$, and consider the extension of splitting fields $L_f/L_g/\mathbb{Q}$ and $L_f/L_h/\mathbb{Q}$. We need $|Z_f| = n$ (because $G \leq S_{Z(f)}$), whence separability. We have a partition $Z_f = Z_g \cup Z_h$. Let $d = \deg(g)$. Since $L_f/\mathbb{Q}$, $L_g/\mathbb{Q}$

Please turn over!

and $L_h/\mathbb{Q}$ are all normal extensions, we have that $\mathrm{Gal}(L_f/\mathbb{Q})/\mathrm{Gal}(L_f/L_g) \cong \mathrm{Gal}(L_g/\mathbb{Q})$ (and similarly for h) via restriction of automorphisms. In particular, automorphisms of L_f restrict to automorphisms of L_g and L_h, so that they permute the roots of g and the roots of h separately. Then the image of G via the embedding in S_n is contained in $S_d \times S_{n-d}$, and the only possibility is that $d = 0$ or $n - d = 0$, so that $f = gh$ is a trivial decomposition. Hence f is irreducible.

2. We claim that $\mathbb{Q}(\alpha)$ cannot contain other roots of f. From this claim, we automatically get that $\mathrm{Aut}(\mathbb{Q}(\alpha)) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha)) = \{\mathrm{id}_{\mathbb{Q}(\alpha)}\}$, because an automorphism of $\mathbb{Q}(\alpha)$ should send α to a root of f lying $\mathbb{Q}(\alpha)$.

   We are then only left to prove that $\mathbb{Q}(\alpha)$ does not contain other roots of f. By previous point, f is the minimal polynomial of α, so that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. Let $g = f/(X - \alpha) \in \mathbb{Q}(\alpha)[X]$. Then $\mathrm{Gal}(L_f/\mathbb{Q}(\alpha)) = [L_f : \mathbb{Q}(\alpha)] = (n-1)!$, and L_f is the splitting field of g over $\mathbb{Q}(\alpha)$. The Galois group $\mathrm{Gal}(L_f/\mathbb{Q}(\alpha))$ fixes all the roots of g lying in $\mathbb{Q}(\alpha)$, and if by contradiction there are $t > 0$ such roots, then the image of this Galois group via the embedding in S_{n-1} lies inside $S_1 \times \cdots \times S_1 \times S_{n-t}$, where S_1 appears t times. But this is impossible, since $|\mathrm{Gal}(L_f/\mathbb{Q}(\alpha))| = (n-1)!$.