1. The wreath product

By a permutation group we mean a group $G$ together with a $G$-set $X$. An embedding of permutation groups $(G, X) \to (G', X')$ is an injective group homomorphism $G \to G'$ together with a bijection $X \to X'$ which is $G$-equivariant. When a group $G$ acts on a set $Y$ we denote the image of $G$ in $\text{Sym}(Y)$ by $G|_Y$.

Suppose that $(G, X)$ and $(H, Y)$ are permutation groups. Then the product group $G \times Y = \text{Map}(Y, G)$ acts on $X \times Y$, by acting only on the first coordinate: we have $f(x, y) = (f(y)x, y)$ for all $x \in X$, $y \in Y$ and $f \in \text{Map}(Y, G)$. The group $H$ acts on $X \times Y$ by acting only on the second coordinate. The group $H$ also acts on $G \times Y$ by permuting coordinates: $(hf)(y) = f(h^{-1}(y))$ when $h \in H$, $y \in Y$ and $f \in \text{Map}(Y, G)$. Thus the semidirect product $G \times Y \rtimes H$ acts on $X \times Y$. This permutation group is called the wreath product of $(G, X)$ and $(H, Y)$ and it is denoted by $G \wr H$.

Let $(G, Z)$ be a permutation group and suppose that $p: Z \to Y$ is a surjective map of $G$-sets, with $Y$ transitive. We define $W$ to be the subgroup of $\text{Sym}(Z)$ that consists of all permutations $w$ of $Z$ that satisfy two conditions:

- $w$ permutes the fibers of $p$ and the induced element of $\text{Sym}(Y)$ lies in $G|_Y$;
- on each fiber of $p$ the map $w$ is multiplication by some element of $G$.

The first condition says $\exists g \in G \forall z \in Z: p(w(z)) = gp(z)$, and the second condition is $\forall y \in Y \exists g \in G \forall z \in p^{-1}(y): w(z) = gz$.

Clearly, $W$ is a permutation group on $Z$, and $G|_Z$ is a permutation subgroup of $W$. Let $H \subset G$ be the stabilizer of a point $y_0 \in Y$ and put $X = p^{-1}(y_0)$.

**Theorem 1.** The permutation group $(W, Z)$ is isomorphic to $H|_X \wr G|_Y$. The permutation group $(G|_Z, Z)$ can be embedded in $H|_X \wr G|_Y$.

Let us sketch the proof. Choose a right-inverse $s: Y \to G$ of the surjective map $G \to Y$ given by $g \mapsto gy_0$, so we have $s(y)y_0 = y$ for all $y \in Y$. Now consider the map $X \times Y \to Z$ given by $(x, y) \mapsto s(y)x$. Note that for each $y \in Y$ the image of $X \times \{y\}$ in $Z$ is $s(y)X = p^{-1}(y)$. It follows that the map is a bijection and it gives rise to an embedding $H|_X \wr G|_Y \to \text{Sym}(Z)$. To show that its image is contained in $W$ we check that for all $y \in Y$ the
elements \( f \in \text{Map}(Y, H|_X) \) and \( \overline{g} \in G|_Y \) acts on \( s(y)X \) in the same way as some element of \( G \). For \( f \) we may take \( s(y)hs(y)^{-1} \in G \) where \( h \in H \) acts as \( f(y) \) on \( X \), and for \( \overline{g} \) we take \( s(\overline{g}y)s(y)^{-1} \in G \).

To see that the map \( H|_X \wr G|_Y \to W \) is surjective, note first that both surject to \( G|_Y \). It remains to show that any \( w \in W \) which acts trivially on \( Y \) acts on \( Z \) in the same way as some element \( f \in \text{Map}(Y, H|_X) \). To see this, not that for each \( y \) there is a \( g_y \in G \) with \( w(s(y)x) = g_y s(y)x \) for all \( x \in X \). For each \( y \in Y \) the element \( h_y = s(y)^{-1}g_ys(y) \) fixes \( y_0 \), so we have \( h_y \in H \), and we take \( f(y) \) to be the image of \( h_y \) in \( H|_X \). This proves the first statement of the theorem. The second statement is an immediate consequence.

2. The Galois group of a tower of field extensions

Let \( K \) be a field and let \( K \subset L \) be a finite separable field extension. By a normal closure of \( L \) over \( K \) we mean a normal field extension \( N \) of \( K \) that is generated by the images of the \( K \)-embeddings \( L \to N \). The Galois group of \( L \) over \( K \) is the permutation group \( (G_{L/K}, X_{L/K}) \) where \( G_{L/K} \) is the Galois group of a normal closure \( N \) of \( L \) over \( K \), and \( X_{L/K} = \text{Hom}_K(L, N) \) is the \( G_{L/K} \)-set of \( K \)-embeddings of \( L \) into \( N \). Note that the choice of \( N \) does not affect the isomorphism type of \( (G_{L/K}, X_{L/K}) \).

Recall that \( X_{L/K} \) is a transitive \( G_{L/K} \)-set whose cardinality is the degree of \( L \) over \( K \). We can also think of \( X_{L/K} \) as the set of zeroes in \( N \) of a defining irreducible polynomial for \( L \).

Theorem 2. Let \( K \subset L \subset M \) be finite separable field extensions. Then the Galois group \( G_{M/K} \) of \( M \) over \( K \) can be embedded as a permutation group into the wreath product \( G_{M/L} \wr G_{L/K} \).

To see how this follows from the first theorem, first fix a normal closure \( N \) of \( M \) over \( K \) that contains \( L \). Then \( G = \text{Gal}(N/K) \) acts transitively on \( Z = \text{Hom}_K(M, N) \) which has a quotient \( G \)-set \( Y = \text{Hom}_K(L, N) \). Let \( H \) be the stabilizer in \( G \) of the inclusion map \( y_0 \) in \( Y \). Then the fiber \( X \) over \( y_0 \) in \( Z \) is \( \text{Hom}_L(M, N) \), and it has an action of \( H \). Now apply theorem 1 and use that \( (G, Z) \) is the Galois group of \( M \) over \( K \), and that \( (H|_X, X) \) is the Galois group of \( M \) over \( L \) and that \( (G|_Y, Y) \) is the Galois group of \( L \) over \( K \).

Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, Netherlands
E-mail address: desmit@math.leidenuniv.nl