2. Groups acting by group automorphisms [s:gaut]

2.1. **Semi-direct products.** Let G be a group acting on a group N by automorphisms: this means that N is a G-set and further that ${}^g nn' = {}^g n {}^g n'$; or, equivalently, that there is a group homomorphism from G into the group of automorphisms of N. From this data we construct now the *semi-direct product* $N \rtimes G$, which is a group containing both G and N.

As a set it is just the cartesian product $N \times G$, and so a typical element is an ordered pair (n, g). The multiplication is defined by $(n, g)(n', g') := (n {}^g n', gg')$. The map $n \mapsto (n, 1)$, respectively $g \mapsto (1, g)$, defines a monomorphism from N, respectively G, into $N \rtimes G$. We identify N and G with their respective images. Their intersection is trivial and they generate the semi-direct product. While N is a normal subgroup (which explains the use of the $\rtimes$ symbol), not so in general G (in fact, not unless the action is trivial). We have the exact sequence:

$$1 \to N \to N \rtimes G \to G \to 1 \tag{2.1}$$

The action of G on N that we started out with can be recovered from $N \rtimes G$ as the conjugation action of the subgroup G on the normal subgroup N. On the other hand, suppose we start out with a subgroup G and a normal subgroup N of a big group K; consider the conjugation action of G on N; assume that N and G intersect trivially and that they generate K. Then $K = NG \simeq N \rtimes G$.

[sss:dn]

2.1.1. An example. Let the group $\mathbb{Z}/2\mathbb{Z}$ act on a cyclic group C by ${}^y x := x^{-1}$, where y is the non-trivial element in $\mathbb{Z}/2\mathbb{Z}$ and x is any element of C. The resulting semi-direct product $C \rtimes \mathbb{Z}/2\mathbb{Z}$ is the *Dihedral group* denoted D_n, where n is the order of C (the cases $n = \infty$ and $n = 1$ are included in these considerations). The action is trivial if $n = 1$ or $n = 2$: we have $D_1 = \mathbb{Z}/2\mathbb{Z}$ and $D_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

The presentation $\langle x, y \,|\, x^n = 1, y^2 = 1, yxy^{-1} = x^{-1} \rangle$ defines D_n, where of course the first relation is understood to be absent when $n = \infty$. Setting $z = xy$ we get another presentation $\langle z, y \,|\, z^2 = 1, y^2 = 1, (zy)^n = 1 \rangle$, which leads to the following alternative definition: a *dihedral group* is a group generated by two involutions.[3] The subscript n in the notation D_n is recovered here as the order of the product of the two involutions.

2.2. **Exercises.**

2.2.1. Consider the action of a group G on itself by left multiplication. Denote by λ_G the image of G under the group homomorphism $\lambda : G \to \operatorname{Bij} G$ defining the above action. The group of automorphisms $\operatorname{Aut} G$ is imbedded naturally as a subgroup in $\operatorname{Bij} G$; it normalizes λ_G: ${}^\varphi \lambda_g = \lambda_{\varphi(g)}$ for $\varphi \in \operatorname{Aut} G$ and $g \in G$. The semi-direct product $\lambda_G \rtimes \operatorname{Aut} G$ is called the *holomorph* of G. Compute the holomorph of a cyclic group.

[sss:genquart]

2.2.2. In the definition of the dihedral group in §2.1.1, let $n = 2t$ be finite and even, pull the action back to $\mathbb{Z}/4\mathbb{Z}$ via the natural epimorphism $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, and consider the semi-direct product $S := \mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$. Denoting by j a generator of $\mathbb{Z}/4\mathbb{Z}$, the centre of S is $\{1, x^t, j^2, x^t j^2\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The quotient of S by the subgroup $\{1, x^t i^2\}$ is the group Q_t of *generalized quarternions*. Its order is $4t$. Every element of Q_t can be written uniquely as $x^e j^f$ with $0 \leq e < 2t$, $0 \leq f \leq 1$. In

[3] The dictionary meaning of the adjective dihedral is: *having or contained by two plane faces*. The generating involutions z and y are the reflections in the two plane faces.

the special case $t = 4$, writing, more suggestively, i and -1 in place respectively of x and x^2, we see that Q_4 is the familiar group of order 8 consisting of the quarternions ± 1, $\pm i$, $\pm j$, $\pm k$.

The subgroup $\langle x \rangle$ of Q_t is normal and cyclic of order $2t$ with $Q_t/\langle x \rangle \simeq \mathbb{Z}/2\mathbb{Z}$. But Q_t is not a semi-direct product of an action of $\mathbb{Z}/2\mathbb{Z}$ on $\mathbb{Z}/2t\mathbb{Z}$: indeed any such semi-direct product would have (at least) two involutions (the images of the unique involutions in $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/2t\mathbb{Z}$) but there is only involution in Q_t, namely x^t.

[ss:ext]

2.3. **Extensions.** An exact sequence of groups like

$$1 \to N \to K \to G \to 1 \tag{2.2}$$

is called an *extension* of G by N. We often say loosely that K is an extension (of G by N). Identifying N with its image in K, we consider N to be a subgroup of K. Being the kernel of the group homomorphism $K \to G$, it is a normal subgroup. The extension is called *central* if N lies in the centre of K. It is called *abelian* (respectively, *cyclic*) if N is abelian (respectively, cyclic).

An extension as above is *split* if there is a group homomorphism $\varphi : G \to K$ which when followed by the epimorphism $K \to G$ gives the identity of G. Such a map φ is called a *splitting*. The extension (2.1) we get from the semi-direct product construction is split: the map $g \mapsto (1, g)$ is evidently a splitting. Conversely, every split extension arises as the extension (2.1) attached to a semi-direct product. Indeed, let φ be a splitting. Then φ is a monomorphism. Identifying G with its image in K under φ, we consider G to be a subgroup of K. It intersects N trivially and together with N generates the group K. Thus $K \simeq N \rtimes G$. To summarise:

(2.3) Split extensions are the same as semi-direct products.

It is easy to give examples of non-split extensions:

$$0 \to p\mathbb{Z}/p^2\mathbb{Z} \subseteq \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0 \tag{2.4}$$

$$0 \to \mathbb{Z} \to \mathbb{R} \to \mathbb{R}/\mathbb{Z} \to 0 \tag{2.5}$$

$$1 \to \langle x \rangle \to Q_t \to \mathbb{Z}/2\mathbb{Z} \to 0 \tag{2.6}$$

where $\langle x \rangle$ and Q_t in (2.6) are as in §2.2.2. It is interesting to formulate criteria under which extensions necessarily split. We state without proof:

[t:schurzhaus]

Theorem 2.1. (Schur-Zassenhaus) *The extension (2.2) splits if the orders of N and G are finite and coprime.*