Semidirect products

August 5, 2016

If G is built out of H and K, we might want to require

1. $H \leq G$, $K \leq G$
2. $HK = \langle hk : h \in H, k \in K \rangle = G$
3. $H \cup K = \{e\}$

Let's try just "taking the union" of two group presentations.

$$\mathbb{Z}/2 * \mathbb{Z}/2 = \langle x, e | x^2 = e \rangle * \langle y, e | y^2 = e \rangle = \langle x, y | x^2 = y^2 = e \rangle$$

which is, upsettingly, an infinite group (note that $(xy)^m \neq (xy)^n$ for $m \neq n$).

We'll let this lead us to a definition:

Definition 1. If $H = \langle H_g | H_r \rangle$ and $K = \langle K_g | K_r \rangle$, then their *free product* is

$$H * K := \langle H_g \cup K_g | H_r \cup K_r, e_H = e_R \rangle$$

.

Now note that the group we were hoping to get ($\mathbb{Z}/2 \times \mathbb{Z}/2 \cong V_4$, the Klein four-group) is recoverable as a quotient:

$$\mathbb{Z}/2 * \mathbb{Z}/2/\langle xy = yx \rangle \cong V_4$$

(this is in fact abelianization, in this special case).

Theorem 1. If G satisfies the three relations at the beginning, it is isomorphic to a quotient of $H * K$.

Proof. By the first isomorphism theorem, this is equivalent to a surjective homomorphism going from $H * K$ to G. Define $\varphi : H * K \to G$ by defining it to be the identity

$$\varphi(h) = h, \varphi(k) = k \ \forall h \in H, k \in K$$

on the subgroups $H, K \leq G$. Now extend this to all other words in the group by imposing the homomorphism condition.

This is easily checked to be surjective, and we are done. □

0.1 The direct product

Given $\{H_i\}_{1,\dots,r}$, the direct product $\prod H_i$ is the group whose elements are of the form $(h_i)_i, h_i \in H_i$, and multiplication is defined elementwise.

Theorem 2. Let $G = \prod G_i$. Then

1. The G_i embed "sanely" into G:
$$G_i \trianglelefteq G.$$
2. Cardinalities work out.
$$|G| = \prod |G_i|.$$
3. The G_i are recoverable from G:
$$G_i \cong \frac{G}{G_1 \times \cdots \times \hat{G}_i \times \cdots \times G_r}.$$

Proof. Well-known. □

Theorem 3. If $H, K \trianglelefteq G$, $H \cap K = \{e\}$, and $HK = G$, then $G \cong H \times K$.

Proof. Notice that

$$\begin{aligned}[h,k] &= hkh^{-1}k^{-1} \\ &= h(kh^{-1}k^{-1}), \text{so } [h,k] \in H \\ &= (hkh^{-1})k^{-1}, \text{so } [h,k] \in K \\ &= e.\end{aligned}$$

Now take $\varphi : H \times K \to G$ sending $(h,k) \mapsto hk$ which is a homomorphism because H and K commute, and an isomorphism because $HK = G$. $\square$

Theorem 4 (Structure theorem for finitely generated abelian groups)**.** If G is an f.g. abelian group,

$$G \simeq \mathbb{Z}^r \times \mathbb{Z}/p_1^{n_1} \times \cdots \times \mathbb{Z}/p_k^{n_k}$$

where r is unique and the (p_i, n_i) are unique up to permutation.

1 Day 2

1.1 Random theorem about dihedral groups

Theorem 5. Let D_{4n} be the symmetries of an n-gon, n odd. Then

$$D_{4n} \cong D_{2n} \times \mathbb{Z}/2$$

Proof. As is well-known,

$$D_{4n} = \langle r, s | r^{2n} = s^2 = (sr)^2 = 1\rangle$$

Now consider the subgroups

$$H = \langle r^2, s\rangle, K = \langle r^n\rangle \subset D_{4n}$$

- H has index 2, and is therefore normal. (The two cosets are H and rH.)
- For K, note that $sr^n s = srssrssrss \cdots rsss = (srs)^n s$

$\square$

Now suppose that $H \trianglelefteq G, K \leq G, H \cap K = \{e\}, HK \leq G$.

Proposition 1. Given these assumptions, every element of HK can be written uniquely as hk for $h \in H, k \in k$.

Proof. Note that $h_1k_1 = h_2k_2 \implies h_2^{-1}h_1 = k_2k_1^{-1} = e$, so we have uniqueness. For existence, consider

$$kh = khk^{-1}k = h'k, h' \in H \trianglelefteq G$$

Given any long string, this gives us a way to "pull all elements of K to the right".

This gives HK the same underlying set as $H \times K$, but the operation is different, in order to sidestep the non-normality (wlog) of K:

$$(h_1k_1) \cdot (h_2k_2) := h_1(k_1h_2k_1^{-1})k_1k_2.$$

$\square$

Definition 2. The *automorphism group* of a group G, $\mathrm{Aut}(G)$, is the group of isomorphisms $G \to G$, where the operation is composition.

Example 1. $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^\times$.

Theorem 6. Let H, K be groups, $\varphi : K \to \mathrm{Aut}(H)$ a group hom, G be the set of pairs (h,k). Define the operation

$$(h,k)(h',k') = (h\varphi(k)(h'), kk').$$

1. This makes G a group with order $|H| \cdot |K|$.
2. (H, e) and (e, K) are subgroups (where one hopes the notation will be self-explanatory) that are isomorphic to H and K respectively.

3. With this identification,

    (a) $H \trianglelefteq G$

    (b) $H \cap K = \{e\}$

    (c) For all $h \in H, k \in K$, $khk^{-1} = \varphi(k)(h)$

We denote this group $H \rtimes_\varphi K$.

Proof. Most of the cases are ones where there is essentially only one way to proceed, and it is a good idea to run through them mentally. $\square$

Theorem 7. If $H \trianglelefteq G, K < G, H \cap K = 1$, and if $\varphi : K \to \mathrm{Aut}(G)$ is conjugation, then $HK \cong H \rtimes K$.

Proposition 2. If H, K are groups, and $\varphi : K \to \mathrm{Aut}(G)$, TFAE:

1. The identity set-function $H \rtimes K \to H \times K$ is a homomorphism.

2. φ is the trivial map.

3. $K \trianglelefteq H \rtimes K$.

Let H be abelian, $K = \mathbb{Z}/2$, let $\varphi : K \to \mathrm{Aut}(H)$ send $\varphi(1)$ to $\varphi(1)(x) = x^{-1}$. This gives a way to make $H \rtimes \mathbb{Z}/2$, when H is cyclic, this is dihedral.

Also:

- $\mathbb{Z}/n \rtimes \mathbb{Z}/2 \cong D_n$

If $|G| = pq$, $p < q$ both prime, then

$$\exists P \leq G, Q \trianglelefteq G, |P| = p, |Q| = q$$

(by Sylow theorems), $P \cap Q = \{e\}$, so

$$G \cong Q \rtimes P \cong \mathbb{Z}/q \rtimes \mathbb{Z}/p$$

We need a $\phi : \mathbb{Z}/p \to \mathrm{Aut}(\mathbb{Z}/q)$, which exists iff $p | q - 1$. If not, $G \cong \mathbb{Z}/pq$.

1.2 Amalgamated free products

Let $H \leq G, K \leq G, H \cap K = N'$.

$$\begin{array}{ccc} N' & \longrightarrow & K \\ \downarrow & & \downarrow f_2 \\ H & \xrightarrow{f_1} & H * K/N \end{array}$$

where

$$N = \langle f_1(n) f_2(n)^{-1} | n \in N' \rangle$$

Now let $H \trianglelefteq G, K \twoheadleftarrow G, H \cap K = \{e\}$. ???

Consider short exact sequences of the form

$$1 \longrightarrow A \xrightarrow{i} E \xrightarrow{\pi} G \longrightarrow 1.$$

with G, A, E finite, A abelian. This is called an extension of G by A.

Given this, we get an action of G on A as follows:

For each $g \in G$, let $e_g = \pi^{-1}(g)$. e_g acts on $i(A)$ by conjugation $e_g i(a) e_g^{-1}$ since $i(A) \trianglelefteq E$ and $A \simeq i(A)$, so e_g acts on A. Any other element in $\pi^{-1}(g)$ is of the form $e_g i(a)$ since

$$e_g i(a') i(a) (e_g i(a'))^{-1} = e_g i(a' a a'^{-1}) e_g^{-1} = e_g i(a) e_g^{-1}$$

Given two extensions, they are equivalent if $\exists \beta : E_1 \to E_2$ such that

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & E_1 & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow & & \| & & \\ 1 & \longrightarrow & A & \longrightarrow & E_2 & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

commutes.

Proposition 3. Equivalent extensions give the same G-module structure on A.

Definition 3. Given a G-module A, a function $f : G \times G \to A$ is a 2-*cocycle* if

$$f(g,h) - g \cdot f(h,k) + f(gh,k) - f(g,hk) = 0.$$

Definition 4. Given a G-module A, a function $f : G \times G \to A$ is a 2-*coboundary* if $\exists f_1 : G \to A$ such that

$$f(g,h) = g \cdot f_1(h) - f_1(gh) + f_1(g).$$

Note that $B^2(G,A) \trianglelefteq H^2(G,A)$. We define, as one would expect, the second group cohomology

$$H^2(G,A) \cong \frac{Z^2(G,A)}{B^2(G,A)}.$$

Theorem 8. There exists a bijection

$$\{\text{equivalence classes of extensions } E\} \longleftrightarrow H^2(G,A)$$

and the identity of $H^2(G,A)$ corresponds to direct products.