$\pi(X \times Y)$ and $\pi(\mathcal{K})$; Semi-Direct Products

Richard Koch

January 29, 2006

1 Group Products

Recall that if H and K are groups, the new group $H \times K$ is the set of all ordered pairs (h, k) with $h \in H$ and $k \in K$. The group operation is

$$(h_1, k_1)(h_2, k_2) = (h_1 h_2, k_1 k_2).$$

2 $\pi(X \times Y)$

On Friday we proved that $\pi(X \times Y)$ is isomorphic to $\pi(X) \times \pi(Y)$. Our conversation was interesting but it made the proof *much* harder than it needs to be.

Let the curve $\gamma(u)$ represent an element of the fundamental group $\pi(X \times Y, x_0 \times y_0)$. Then

$$\gamma(u) = (x(u), y(u))$$

where $x(u)$ and $y(u)$ are the components of $\gamma(u)$ in X and Y. Since $\gamma(u)$ starts and ends at (x_0, y_0), $x(u)$ starts and ends at x_0 and $y(u)$ starts and ends at y_0. So $x(u)$ represents an element of $\pi(X, x_0)$ and $y(u)$ represents an element of $\pi(Y, y_0)$.

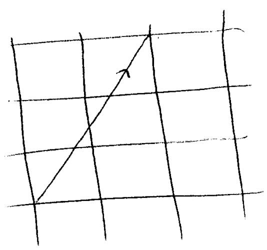
Two paths $\gamma_1(u)$ and $\gamma_2(u)$ represent the same element just in case they are homotopic. Such a homotopy is a map $H : I \times I \to X \times Y$ with the correct boundary conditions. This map can be written $H(u, t) = (h(u, t), k(u, t))$ where h and k are the components of H in X and Y; notice that $h : I \times I \to X$ and $k : I \times I \to Y$. Consequently a homotopy between two curves in $X \times Y$ is just a pair of homotopies between their X and Y components. It follows immediately that an element of $\pi(X \times Y)$ is just a pair of elements, one in $\pi(X)$ and the other in $\pi(Y)$.

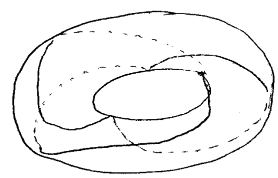
The resulting one-to-one correspondence between $\pi(X \times Y)$ and $\pi(X) \times \pi(Y)$ preserves the group operation, because when we multiply $\gamma_1(u) = (x_1(u), y_1(u))$ and $\gamma_2(u) = (x_2(u), y_2(u))$

we first do γ_1 and then do γ_2; looking at the X component, we first do x_1 and then do x_2, and similarly with the second component.

This completes the argument!

For example, $\pi(S^1 \times S^1) = \pi(S^1) \times \pi(S^1) = Z \times Z$. Consider the element $(2,3) \in Z \times Z$. Usually we take as representatives the map which wraps the circle around itself twice at uniform speed, and the map which wraps the circle around itself three times at uniform speed. The resulting representative in the torus is a helix which simultaneously wraps in both directions.



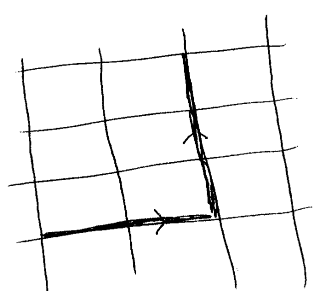


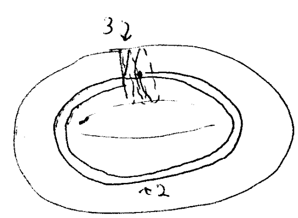
best I can do

Sometimes, however, it is nice to think of $(2,3)$ in the torus another way, as a map which wraps around the first circle twice without wrapping around the second circle at all, followed by a map which wraps around the second circle three times without wrapping around the first circle at all. It is easy to see that this is another representative of $(2,3)$. Indeed the discussion on page one shows that we are free to change the representatives in $\pi(X)$ and $\pi(Y)$ independently. Let us replace $x(u)$ with $x(u) \star x_0$; these are homotopic by the argument that $\pi(X)$ has a group identity. Let us replace $y(u)$ with $y_0 \star y(u))$. Then

$$(x(u), y(u)) \sim (x(u) \star x_0, y_0 \star y(u)) \sim (x(u), y_0) \star (x_0, y(u))$$

This last map clearly wraps around the first circle, and then wraps around the second circle.



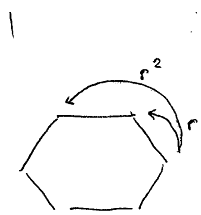


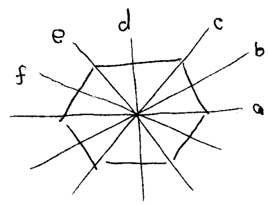
ditto

3 Basic Philosophy of Group Theory

One of the central ideas in group theory is that complicated groups G are often built of easier groups H and K. For instance, we can construct $G = H \times K$ from H and K; as we'll see, other groups can also be built from H and K. Group theory then consists of listing the "irreducible" groups that cannot be broken into smaller pieces, and then studying ways to put groups together.

For example, consider the dihedral group D_n of all rotations and reflections of a regular n-sided polygon. This group consists of rotations of the polygon (which form a subgroup isomorphic to Z_n) and of n reflections. Each reflection generates a subgroup isomorphic to Z_2 since reflecting twice about the same axis gives the identity. So in some sense D_n is constructed from Z_n and Z_2.





$D_6 = \{e, r, r^2, r^3, r^4, r^5, a, b, c, d, e, f\}$

After much trial and error, the group theorists found a very elegant way to discuss constructing G from easier H and K. In this approach H and K are not treated symmetrically; instead the crucial first step is to find an onto group homomorphism $r : G \to K$. Then we define H to be the set of all $g \in G$ such that $r(g) = e$. This is easily seen to be a subgroup of G which group theorists call it the kernel of r. We get a diagram

$$0 \to H \xrightarrow{i} G \xrightarrow{r} K \to 0$$

In general a sequence of group homomorphisms $H \xrightarrow{i} G \xrightarrow{r} K$ is said to be *exact at* G if $g \in G$ comes from H exactly when it maps to $e \in K$. The short exact sequence displayed above is exact at H because i is one-to-one, exact at G by definition of H, and exact at K because r is onto.

In the dihedral case, define $r : D_n \to Z_2$ to be the map which sends rotations to $0 \in Z_2$ and reflections to $1 \in Z_2$. This is a group homomorphism because the product of a rotation and a reflection is another reflection and the product of two reflections is a rotation. If elements of D_n are represented by 2×2 matrices, then this homomorphism is $A \to \det(A)$ because the determinant of a distance preserving map is ± 1; in this case Z_2 is the multiplicative group $\{1, -1\}$.

(Group theorists are smart. In the dihedral case, there is a canonical $r : D_n \to Z_2$, although there are many subgroups K isomorphic to Z_2. So the essential point is $r : G \to K$ rather than copies of K in G.)

Given G, it may happen that the only onto homomorphisms starting at G are the zero map which sends everything to e and the identity map which sends G to itself. In that case one of H and K is $\{e\}$ and the other is G and it is impossible to break G into smaller pieces. Such a G is called a *simple group.* The finite abelian simple groups are exactly Z_p for p prime. There are infinitely many finite nonabelian simple groups. The smallest is the group of all rotations of a dodecahedron (this group has 60 elements); thus it is fitting that the symbol of the Mathematical Association of America is a dodecahedron. One of the greatest accomplishments of the twentieth century is a complete classification of all finite simple groups. Most of these groups lie in several infinite families: for example, the alternating groups A_n of all even permutations on n letters are simple when $n \geq 5$, and the matrix groups $SL(n, F)$ modulo diagonal matrices are simple for most finite fields F. There are also 26 simple groups which do not fit into such families; they are called the sporadic simple groups.

This complete classification was announced in 1983 by Danny Gorenstein, who had outlined a program for approaching the classification several years earlier. It is estimated that the complete proof takes about 30,000 pages. However, in 1983 when the announcement was made, there was a missing step in the proof. This missing step was only filled in 2004 by Michael Aschbacher and Stephen Smith, in two volumes totaling 1221 pages. So the classification of finite simple groups is a *recent* accomplishment!

Luckily, we don't need to understand simple groups in our course. But we do need to know something about breaking groups into smaller pieces.

4 Split Sequences

Suppose G is built from H and K in the sense that we have an onto homomorphism $r : G \to K$ and thus a short exact sequence

$$0 \to H \xrightarrow{i} G \xrightarrow{r} K \to 0$$

By definition, the group H is a subgroup of G. But the group K need not be a subgroup of G; said more precisely, there need not be a subgroup $\tilde{K}$ of G mapped isomorphically to K by r.

For example, consider the group of unit quaternions $\{\pm 1, \pm i, \pm j, \pm k\}$ where $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$, $jk = -kj = i$, and $ki = -ik = j$. Map this group to $Z_2 \times Z_2$ by sending ± 1 to $(0, 0)$, $\pm i$ to $(1, 0)$, $\pm j$ to $(0, 1)$, and $\pm k$ to $(1, 1)$. It is easy to see that this is a group homomorphism. The kernel of this homomorphism is Z_2, so according to our philosophy, the full group is built from Z_2 and $Z_2 \times Z_2$.

However, no subgroup of the full group is isomorphic to $Z_2 \times Z_2$ since the only elements in the full group satisfying $g^2 = e$ are ± 1, while all four elements of $Z_2 \times Z_2$ satisfy this condition.

We say the sequence

$$0 \to H \xrightarrow{i} G \xrightarrow{r} K \to 0$$

splits if there is a group homomorphism $s : K \to G$ such that $r \circ s : K \to K$ is the identity. This is a fancy way of saying that we can think of K as the image $s(K) \subset G$ and thus regard K as a subgroup of G. The quaterionic example just given shows that some sequences do not split.

The dihedral case does split: $0 \to Z_n \xrightarrow{i} D_n \xrightarrow{r} Z_2 \to 0$. Indeed, we can map Z_2 to D_n by sending $1 \in Z_2$ to any of the reflections in the group.

In topology split sequences arise naturally from retractions. If $r : X \to A$ is a retraction, we have a sequence

$$0 \to \mathrm{Ker}(r_\star) \to \pi(X) \xrightarrow{r_\star} \pi(A) \to 0$$

and there is a natural one-to-one map $\pi(A) \to \pi(X)$ because $A \to X \to A$ is the identity map.

In our course it suffices to understand the easier case when the sequence splits. We will do that case in the next couple of pages. We are going to discover that when the sequence splits, G is completely determined by H and K and *one other piece of information.* When we apply this to the fundamental group, we'll discover that this other piece of information arises in a beautiful topological manner.

5 Group Theory of Split Sequences

Theorem 1 *Suppose the sequence*

$$0 \to H \xrightarrow{i} G \xrightarrow{r} K \to 0$$

splits. Identify K with a subgroup of G via the splitting map $s : K \to G$. Then every element of $g \in G$ can be written uniquely in the form

$$g = hk$$

with $h \in H$ and $k \in K$.

Proof: This representation is unique, for if $h_1k_1 = h_2k_2$, then $r(g) = r(h_1k_1) = r(h_1)r(k_1) = k_1$ and similarly $r(g) = k_2$, so $k_1 = k_2$, and then $h_1 = h_2$.

The representation exists, for if $g \in G$ let $k = r(g)$ and write $g = (gk^{-1})k$. Notice that $gk^{-1} \in H$ because $r(gk^{-1}) = r(g)r(k)^{-1} = kk^{-1} = e$.

Theorem 2 *If the sequence* $0 \to H \xrightarrow{i} G \xrightarrow{r} K \to 0$ *splits and thus every element is a product* hk*, then the group law on these products is*

$$(h_1k_1)\ (h_2k_2) = (h_1 \circ k_1h_2k_1^{-1})\ (k_1k_2)$$

Proof: Clearly $(h_1k_1)(h_2k_2) = (h_1k_1h_2k_1^{-1})(k_1k_2)$. In this expression, notice that $k_1h_2k_1^{-1}$ belongs to H since it is in the kernel of r. Indeed $r(k_1h_2k_1^{-1}) = r(k_1)r(h_2)r(k_1^{-1}) = r(k_1) \circ e \circ r(k_1)^{-1} = e$. Consequently the expression inside the first parentheses is the component of the product in H and the expression inside the second parenthesis is the component of the product in K.

6 Fundamental Data

We want to restate the results in the previous section using only H and K, and explain how to construct G from this data without knowing G in advance. It turns out that we need to know one more thing:

Definition 1 *An automorphism of a group* H *is a group homomorphism* $\varphi : H \to H$ *which is one-to-one and onto. The set of all automorphisms of* H *forms a group under composition; this group is called* $Aut(H)$.

Example 1 *Let* $\varphi : Z \to Z$ *be an automorphism. The group* Z *has two generators:* ± 1. *Since automorphisms preserve everything, they must map generators to generators. So either* $\varphi(1) = 1$ *or else* $\varphi(1) = -1$. *In the first case* $\varphi(n) = n$ *for all* n *and* φ *is the identity map. In the second case,* $\varphi(n) = -n$ *for all* n. *It follows that* $Aut(Z) = Z_2$.

Theorem 3 *Suppose that* $0 \to H \xrightarrow{i} G \xrightarrow{r} K \to 0$ *is split. The map* $\phi : K \to Aut(H)$ *defined by* $\phi_k(h) = khk^{-1}$ *is a group homomorphism from* K *to the group of automorphisms of* H.

Proof: This is easily checked.

Definition 2 *Suppose H and K are groups and $\phi : K \to Aut(H)$ is a group homomorphism. Define a new group $H \rtimes_\phi K$, called the* semidirect product of H and K*, by letting*

$$H \rtimes_\phi K = H \times K$$

as a set, and defining

$$(h_1, k_1) \circ (h_2, k_2) = (h_1 \phi_{k_1}(h_2), k_1 k_2)$$

Remark: It is easy to show that this semidirect product is indeed a group.

Theorem 4 *Let*

$$0 \to H \xrightarrow{i} G \xrightarrow{r} K \to 0$$

be a split short exact sequence. Define $\phi : K \to Aut(H)$ as in theorem 3. Then G is isomorphic to

$$H \rtimes_\phi K$$

Proof: Easy.

Remark: Thus one way to construct a group G from smaller pieces H and K is to find a homomorphism $\phi : K \to Aut(H)$ and let $G = H \rtimes_\phi K$. The arguments just given show that every split exact sequence arises in this way. Certainly there is one obvious map $K \to Aut(H)$, namely the map that sends every element to the identity element. The resulting semidirect product is the product $H \times K$. It may happen that this is the only homomorphism $K \to Aut(H)$. But there may be more, and then we can construct other G from H and K.

Remark: Define $\varphi : Z_n \to Z_n$ by $\varphi(k) = -k$. This is clearly an automorphism. Moreover, ϕ^2 is the identity. So there is a homomorphism $\phi : Z_2 \to Aut(Z_n)$ by letting the nonzero element of Z_2 map to φ. It is easy to see that

$$D_n = Z_n \rtimes_\phi Z_2.$$

7 Semidirect Products of Z and Z

As a special case, consider split exact sequences of the form

$$0 \to Z \to G \to Z \to 0$$

Such a sequence induces a group homomorphism $Z \to Aut(Z)$. This homomorphism is completely determine by the image of the generator $1 \in Z$. Since $Aut(Z) = Z_2$, the generator can either go to the identity map or to the map $\varphi(n) = -n$. In the first case, the semidirect product is the ordinary product $Z \times Z$. In the second case, $\phi_k(n) = n$ for k even and $\phi_k(n) = -n$ for k odd. We easily write down the general group law:

$$(m_1, n_1) \circ (m_2, n_2) = (m_1 + (-1)^{n_1} m_2, n_1 + n_1)$$

Notice that $Z \times Z$ is abelian and $Z \rtimes_\phi Z$ is not abelian. Thus if $H = K = Z$, there are exactly two G which can be constructed giving rise to a split sequence.

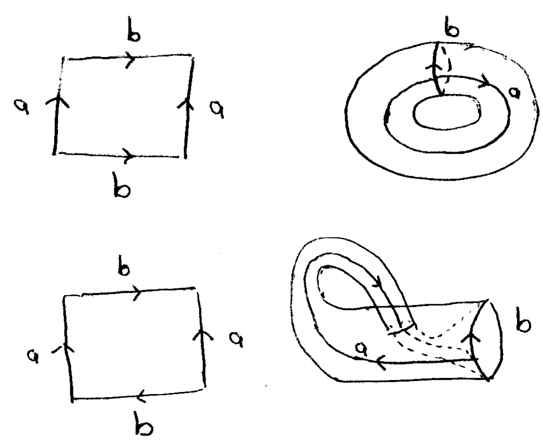
It is easy to show that when $K = Z$ the sequence automatically splits. So we can construct exactly two groups starting with two copies of Z.

8 Application to Topology

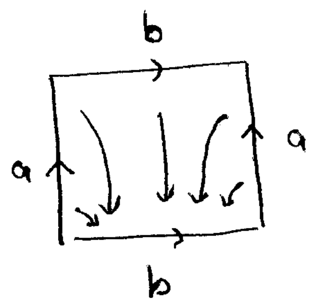
Consider the torus $S^1 \times S^1$ and the Klein bottle $\mathcal{K}$. In both cases there are two obvious closed paths, indicated by a and b in the pictures below. In both cases, there is a retraction r from the full X to the image $A \subseteq X$ of the path a. The fundamental group of A is Z, so we get an exact sequence

$$0 \to H \to \pi(X) \to Z \to 0$$

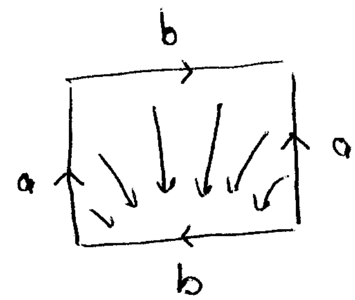
where $H = \mathrm{Ker}(\pi(X) \xrightarrow{r_\star} \pi(A))$. Since $r(b)$ is a single point, the image of b is certainly in this kernel. One can prove that the kernel is exactly Z with generator b, although we do not yet have the power to do so in the case of the Klein bottle.



It follows that $\pi(X)$ is one of two groups, $Z \times Z$ or $Z \rtimes_\phi Z$. To determine which of these groups occurs, we must find the homomorphism $K \to Aut(H)$. The group $K = Z$ is generated by a, and the group $H = Z$ is generated by b, so we must compute $\phi_a(b) = aba^{-1}$. The pictures below show that this element is b for the torus and b^{-1} for the Klein bottle. It immediately follows that $\pi(S^1 \times S^1) = Z \times Z$, as we proved directly in the first section of these notes, and $\pi(\mathcal{K}) = Z \rtimes_\phi Z$.



T^2



$\mathcal{K}$