

CONTENTS

1. Products of cyclic groups	1
2. Internal direct products	2
3. Quotient groups	4

Last time we introduce the notion of an external direct product of two groups. If G_1 , and G_2 are two groups, this is defined as the set

$$G_1 \times G_2 \tag{0.1}$$

equipped with componentwise multiplication. The identity is (e_{G_1}, e_{G_2}) and the inverse of (g_1, g_2) is (g_1^{-1}, g_2^{-1}) .

1. PRODUCTS OF CYCLIC GROUPS

Write C_d for a cyclic group of order d .

Lemma 1.1. *If $r, s \geq 1$ and $\gcd(r, s) = 1$, then*

$$C_{rs} \cong C_r \times C_s.$$

Warning

The coprimality assumption matters. For example, $C_4 \not\cong C_2 \times C_2$. Every element (u, v) of $C_2 \times C_2$ satisfies

$$(u, v)^2 = (u^2, v^2) = (1, 1),$$

whereas C_4 has an element of order 4. An isomorphism preserves element orders, so these groups cannot be isomorphic.

Proof of Lemma 1.1. Choose generators

$$C_{rs} = \langle x \rangle, \quad C_r = \langle z \rangle, \quad C_s = \langle y \rangle.$$

Define

$$\varphi : C_{rs} \rightarrow C_r, \quad x^i \mapsto z^i, \quad \psi : C_{rs} \rightarrow C_s, \quad x^i \mapsto y^i.$$

These maps are well defined: if $x^i = x^j$, then $rs \mid (i - j)$, so both r and s divide $i - j$, giving $z^i = z^j$ and $y^i = y^j$. They are homomorphisms, since, for instance,

$$\varphi(x^i x^j) = z^{i+j} = z^i z^j.$$

Define a map using these two coordinates:

$$\Phi : C_{rs} \longrightarrow C_r \times C_s, \quad x^i \longmapsto (z^i, y^i).$$

It is a homomorphism because multiplication is componentwise:

$$\Phi(x^i x^j) = (z^{i+j}, y^{i+j}) = (z^i, y^i)(z^j, y^j) = \Phi(x^i)\Phi(x^j).$$

The two coordinate kernels are

$$\ker(\varphi) = \langle x^r \rangle, \quad \ker(\psi) = \langle x^s \rangle.$$

Consequently, $x^i \in \ker(\Phi)$ if and only if $r \mid i$ and $s \mid i$. Since $\gcd(r, s) = 1$, this is equivalent to $rs \mid i$, so $\ker(\Phi) = \{1\}$ and Φ is injective.

Both its domain and its codomain have order rs . Thus Φ is also surjective, and hence an isomorphism. Equivalently, the counting formula gives $|\operatorname{im}(\Phi)| = rs$, so its image is all of $C_r \times C_s$. $\square$

2. INTERNAL DIRECT PRODUCTS

We now take the internal point of view: given subgroups $H, K \leq G$, when can we identify G with $H \times K$ using the multiplication map $(h, k) \mapsto hk$?

2.1. The product of two subgroups. Let $H, K \leq G$. The *product set* of H and K is

$$HK = \{hk \mid h \in H, k \in K\} \subseteq G.$$

Here HK consists of elements of G , whereas $H \times K$ consists of ordered pairs and has the external direct product group structure.

Warning

The set HK need not be a subgroup of G .

Example 2.1. In S_3 , let $H = \langle (12) \rangle$ and $K = \langle (23) \rangle$. Composing permutations from right to left,

$$HK = \{1, (12), (23), (123)\}.$$

This set is not closed under multiplication: both (23) and (12) belong to HK , but their product (132) does not.

Lemma 2.1. *If either H or K is normal in G , then $HK = KH$ and $HK \leq G$.*

Proof. Suppose first that $H \trianglelefteq G$. For $h \in H$ and $k \in K$,

$$hk = k(k^{-1}hk) \in KH, \quad kh = (khk^{-1})k \in HK,$$

because the conjugates $k^{-1}hk$ and khk^{-1} lie in H . Thus $HK = KH$.

The identity lies in HK . For closure under multiplication, write $k_1h_2 = h'_2k'_1$ using $KH = HK$. Then

$$(h_1k_1)(h_2k_2) = (h_1h'_2)(k'_1k_2) \in HK.$$

Also, $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$, so HK is closed under inverses and hence is a subgroup. If $K \trianglelefteq G$, interchange H and K in the argument. $\square$

2.2. Recognizing a direct product.

Definition 2.1 (Internal direct product). A group G is the *internal direct product* of subgroups H and K if

$$H \trianglelefteq G, \quad K \trianglelefteq G, \quad H \cap K = \{1\}, \quad HK = G.$$

Let's begin with a simple lemma.

Lemma 2.2 (Unique factorization). *If $H \cap K = \{1\}$, the multiplication map of sets*

$$p : H \times K \longrightarrow G, \quad (h, k) \longmapsto hk$$

is injective. Thus each element of HK has a unique expression hk with $h \in H$ and $k \in K$.

Proof. If $h_1k_1 = h_2k_2$, then

$$h_2^{-1}h_1 = k_2k_1^{-1}.$$

The left side lies in H and the right side lies in K . Their common value therefore belongs to $H \cap K = \{1\}$, so $h_1 = h_2$ and $k_1 = k_2$. $\square$

Theorem 2.1 (Recognizing direct products). *If G is the internal direct product of H and K , then*

$$G \cong H \times K.$$

The isomorphism sends $g = hk$ to (h, k) .

Proof. Since $HK = G$, every $g \in G$ can be written $g = hk$. By Lemma 2.2, this expression is unique. Hence

$$\pi : G \longrightarrow H \times K, \quad hk \longmapsto (h, k)$$

is well defined.

First we show that elements of H commute with elements of K . For $h \in H$ and $k \in K$, consider the commutator

$$[h, k] = hkh^{-1}k^{-1}.$$

Normality of K gives $hkh^{-1} \in K$, so $[h, k] \in K$. Normality of H gives $kh^{-1}k^{-1} \in H$, so $[h, k] = h(kh^{-1}k^{-1}) \in H$. Consequently,

$$[h, k] \in H \cap K = \{1\}, \quad \text{and thus } hk = kh.$$

Now let $g_1 = h_1k_1$ and $g_2 = h_2k_2$. Since $k_1h_2 = h_2k_1$,

$$g_1g_2 = h_1k_1h_2k_2 = (h_1h_2)(k_1k_2).$$

It follows that

$$\pi(g_1g_2) = (h_1h_2, k_1k_2) = (h_1, k_1)(h_2, k_2) = \pi(g_1)\pi(g_2).$$

Thus π is a homomorphism. It is bijective, with inverse $p(h, k) = hk$, and hence is an isomorphism. $\square$

Exercise 2.2. Verify directly that the maps π and p in Theorem 2.1 are inverses. Then check that the subgroups $\tilde{G}_1$ and $\tilde{G}_2$ of the external product $G_1 \times G_2$ satisfy all four conditions in the definition of an internal direct product.

Remark. Both normality assumptions matter. If only $H \trianglelefteq G$ is assumed, together with $H \cap K = \{1\}$ and $HK = G$, the resulting structure is called a *semidirect product*, written $G \cong H \rtimes K$; the factors need not commute.

For example, in S_3 take $H = \langle a \rangle$ with $a = (1\ 2\ 3)$ and $K = \langle b \rangle$ with $b = (1\ 2)$. Then $H \trianglelefteq S_3$, $H \cap K = \{1\}$, and

$$HK = \{1, a, a^2, b, ab, a^2b\} = S_3.$$

But K is not normal: $aba^{-1} = (2\ 3) \notin K$. Moreover, $bab^{-1} = a^{-1} \neq a$, so the factors do not commute. Thus $S_3 \cong C_3 \rtimes C_2$ is a semidirect product; it is not isomorphic to the abelian group $C_3 \times C_2$.

3. QUOTIENT GROUPS

Let $H \leq G$. Recall that G/H denotes the *set* of left cosets gH . We would like to multiply cosets by the rule

$$(g_1H)(g_2H) = (g_1g_2)H.$$

Before checking the group axioms, we must check that this rule does not depend on the representatives g_1 and g_2 .

3.1. Why normality is needed. If $g'_1 = g_1h_1$ and $g'_2 = g_2h_2$ with $h_1, h_2 \in H$, then $g'_1H = g_1H$ and $g'_2H = g_2H$. But

$$g'_1g'_2 = g_1h_1g_2h_2 = g_1g_2(g_2^{-1}h_1g_2)h_2.$$

If $H \trianglelefteq G$, the parenthesized element lies in H , and therefore $g'_1g'_2H = g_1g_2H$, as required.

Example 3.1 (Failure for a nonnormal subgroup). Take $G = S_3$ and $H = \{1, (12)\}$. The identity coset has both 1 and (12) as representatives. Using $g_2 = (23)$ gives

$$1(23)H = (23)H, \quad (12)(23)H = (123)H.$$

These cosets are distinct: otherwise $(23)^{-1}(123) = (13)$ would belong to H . Thus the proposed product depends on the chosen representative.

Remark. In fact, normality is necessary for this multiplication rule to be well defined. If it is well defined, then for every $h \in H$ and $g \in G$,

$$(hH)(gH) = (1H)(gH), \quad \text{so } hgH = gH.$$

Hence $g^{-1}hg \in H$. Applying this for every g proves $H \trianglelefteq G$.

3.2. The quotient construction.

Theorem 3.1 (Quotient group). *Let $N \trianglelefteq G$. The set G/N is a group under*

$$(gN)(hN) = (gh)N.$$

Its identity is $N = 1N$, and the inverse of gN is $g^{-1}N$.

Proof. The preceding calculation proves that multiplication is well defined. Associativity follows from associativity in G :

$$((gN)(hN))(kN) = ((gh)k)N = (g(hk))N = (gN)((hN)(kN)).$$

Also, $N(gN) = (gN)N = gN$, and

$$(gN)(g^{-1}N) = (g^{-1}N)(gN) = N.$$

These are the group axioms. □

Theorem 3.2 (The quotient map). *The map*

$$\pi : G \longrightarrow G/N, \quad g \longmapsto gN$$

is a surjective homomorphism with kernel N .

Proof. By definition of the quotient multiplication, $\pi(gh) = (gh)N = (gN)(hN) = \pi(g)\pi(h)$. Every coset has a representative, so π is surjective. Finally,

$$g \in \ker \pi \iff gN = N \iff g \in N.$$

□

Corollary 3.1. *If G is finite, then $|G/N| = [G : N] = |G|/|N|$.*

Proof. The elements of G/N are precisely the left cosets of N in G . Each has $|N|$ elements, and they partition G . $\square$

Example 3.2. In additive notation, $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ and

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}.$$

Thus $\mathbb{Z}/n\mathbb{Z}$ is the familiar group of integers modulo n . The quotient map sends an integer to its residue class; its kernel is $n\mathbb{Z}$.

Exercise 3.3. For the external product $H \times K$, show that

$$(H \times K)/(H \times \{1\}) \cong K$$

by defining a map $(h, k)(H \times \{1\}) \mapsto k$. Check that it is well defined and is a bijective homomorphism.