

MATH 30A: CHAPTER 8

8. EXTERNAL DIRECT PRODUCTS

This is a way to make new groups out of old ones.

8.1. definition.

Definition 8.1. *If G_1, G_2, \dots, G_n are groups then the external direct product*

$$G_1 \oplus G_2 \oplus \dots \oplus G_n$$

is defined (in our book) to be the set of all n -tuples (g_1, g_2, \dots, g_n) where $g_i \in G_i$ with multiplication given coordinate-wise:

$$(g_1, g_2, \dots, g_n)(h_1, h_2, \dots, h_n) = (g_1 h_1, g_2 h_2, \dots, g_n h_n)$$

If the groups are additive this is

$$(g_1, \dots, g_n) + (h_1, \dots, h_n) = (g_1 + h_1, \dots, g_n + h_n)$$

Someone asked what happens if some of the groups are multiplicative and some are additive. In that case the operation on the product is multiplication:

$$(a, x)(b, y) = (ab, x + y)$$

if the first group is multiplicative and the second is additive.

8.2. examples. I gave some the standard “obvious” example of \mathbb{R}^2 and the not so obvious example of $\mathbb{Z}_n \oplus \mathbb{Z}_m$.

8.2.1. two dimensional space. If $G = H = \mathbb{R}, +$ then $G \oplus H = \mathbb{R}^2$ is the set of all pairs (x, y) where $x, y \in \mathbb{R}$. Thus the points in the product are points in the Cartesian plane. Addition is vector addition

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

8.2.2. *product of cyclic groups.* An interesting example is:

$$\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$$

An isomorphism $\phi : \mathbb{Z}_6 \rightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_3$ is given by $\phi(x) = (x \bmod 2, x \bmod 3)$. This is a bijection:

$$\phi(0) = (0, 0), \phi(1) = (1, 1), \phi(2) = (0, 2), \phi(3) = (1, 0), \phi(4) = (0, 1), \phi(5) = (1, 2)$$

And it is easy to see that it is operation preserving.

Theorem 8.2. *If n, m are relatively prime then $\mathbb{Z}_n \oplus \mathbb{Z}_m$ is cyclic of order nm .*

In your quiz 2 I asked for a generator of $\mathbb{Z}_{37} \oplus \mathbb{Z}_{101}$. The element $(1, 1)$ is a generator since $3737(1, 1) = (0, 0)$ but $(1, 1)$ does not have order 1, 37 or 101. This means that an isomorphism

$$\phi : \mathbb{Z}_{3737} \xrightarrow{\cong} \mathbb{Z}_{37} \oplus \mathbb{Z}_{101}$$

is given by $\phi(x) = (x \bmod 37, x \bmod 101)$.

Another isomorphism

$$\psi : \mathbb{Z}_{37} \oplus \mathbb{Z}_{101} \xrightarrow{\cong} \mathbb{Z}_{3737}$$

is given by $\psi(x, y) = 101x + 37y$ (modulo 3737).

Then I wanted to know: What is $\phi^{-1}(x, y)$ and what is $\psi^{-1}(x)$?

8.3. Euclidean algorithm.

8.3.1. *Chinese remainder theorem.* In order to find the inverse function for the isomorphism $\phi(x) = (x \bmod 37, x \bmod 101)$ we need to solve the following congruence problems: Given integers a, b find an integer c so that

$$\begin{aligned} c &\equiv a \pmod{37} \\ c &\equiv b \pmod{101} \end{aligned}$$

To do this we need the

Theorem 8.3 (Chinese remainder theorem). *If n, m are relatively prime, there exist integers x, y so that*

$$\frac{1}{nm} = \frac{x}{n} + \frac{y}{m}$$

I.e., $1 = xm + yn$.

This theorem says there are integers x, y so that $101x + 37y = 1$. Then $c = 101xa + 37yb$ is a solution of the congruence problem.

You might recognize the Chinese remainder theorem in this form:

$$\frac{1}{(x-a)(x-b)} = \frac{A}{x-a} + \frac{B}{x-b}$$

To find the numbers x, y in the theorem we need the *Euclidean algorithm*.

8.3.2. *the algorithm*. The Euclidean algorithm is simple: You take two numbers, say a, b . You subtract the smaller number from the larger. (Replace the larger number a with $a - b$.) Keep doing this until you get zero. Then the other number is the greatest common divisor. Instead of subtracting over and over, we usually divide and take remainder. (Replace a with $a \bmod b$.)

For example, take $a = 16, b = 6$. Then the quotient $(16/6)$ is 2 with remainder 4 giving 6, 4. The quotient is now 1 with remainder 2 giving 4, 2. Finally the quotient is 2 with remainder 0 giving 2, 0. Thus $2 = \gcd(16, 6)$. The algorithm also gives numbers x, y so that

$$2 = 16x + 6y$$

This goes using a chart:

x	y	$ax + by$	$quotient$
1	0	$a = 16$	
0	1	$b = 6$	2
1	-2	4	1
-1	3	2	2
		0	

The result is that $2 = 16(-1) + 6(3)$.

For 101 and 37 we get:

x	y	$ax + by$	$quotient$
1	0	$a = 101$	
0	1	$b = 37$	2
1	-2	27	1
-1	3	10	2
3	-8	7	1
-4	11	3	2
11	-30	1	

So, $1 = 11(101) - 30(37) = 1111 - 1110$. The numbers 1111 and -1110 (or 2627) are what we want:

$$\phi^{-1}(a, b) = 1111a + 2627b$$

this is the number which, when reduced modulo 37 gives a and reduced modulo 101 gives b .

8.4. Fundamental theorem of finite abelian groups. In class I talked about *finitely generated* abelian groups. I will explain that again later when it is in the book. The book only does finite abelian groups.

Theorem 8.4 (Fundamental theorem of finite abelian groups). *Every finite abelian group G is isomorphic to a direct product of cyclic groups*

$$G \cong \mathbb{Z}_{t_1} \oplus \mathbb{Z}_{t_2} \oplus \cdots \oplus \mathbb{Z}_{t_s}$$

where each t_i divides the previous one ($t_{i+1} | t_i$). Furthermore, these integers t_i are uniquely determined by G . They are called the torsion coefficients of G .

With this theorem you can classify all the finite abelian groups up to isomorphism. For example, suppose you want to know all abelian groups of order 12. To find these you write 12 as a product of numbers each one dividing the previous. There are only two ways: $12 = 6 \cdot 2$ or $12 = 12 \cdot 1$. So,

$$\mathbb{Z}_6 \oplus \mathbb{Z}_2, \quad \mathbb{Z}_{12}$$

are, up to isomorphism, the only abelian groups of order 12. For 8 there are three ways: $8 = 8 = 4 \cdot 2 = 2 \cdot 2 \cdot 2$. So,

$$\mathbb{Z}_8, \quad \mathbb{Z}_4 \oplus \mathbb{Z}_2, \quad \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 (= (\mathbb{Z}_2)^3)$$

are, up to isomorphism, the only abelian groups of order 8.

8.5. Groups of order ≤ 12 .

#	$ G $	abelian gps	nonabelian gps	comments
1	1	$\{e\}$	—	
1	2	\mathbb{Z}_2	—	gps of order p are cyclic
1	3	\mathbb{Z}_3	—	gps of order p are cyclic
2	4	$\mathbb{Z}_4, \mathbb{Z}_2 \oplus \mathbb{Z}_2$	—	gps of order p^2 are abelian
1	5	\mathbb{Z}_5	—	gps of order p are cyclic
2	6	\mathbb{Z}_6	D_3	gps of order $2p$ are dihedral or cyclic
1	7	\mathbb{Z}_7	—	gps of order p are cyclic
5	8	(three)	D_4, Q	there are 2 nonabelian gps of order p^3
2	9	$\mathbb{Z}_9, \mathbb{Z}_3 \oplus \mathbb{Z}_3$	—	gps of order p^2 are abelian
2	10	\mathbb{Z}_{10}	D_5	gps of order $2p$ are dihedral or cyclic
1	11	\mathbb{Z}_{11}	—	gps of order p are cyclic
5	12	$\mathbb{Z}_{12}, \mathbb{Z}_6 \oplus \mathbb{Z}_2$	$D_4, A_4, \widetilde{D}_3$	by Sylow theorems (Chap 24)

Here Q is the group of *quaternions*

$$Q := \{\pm 1, \pm i, \pm j, \pm k\}$$

with $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k, jk = -kj = i, ki = -ik = j$.

8.6. semidirect product. One other thing I mentioned in class was the semi-direct product which is a twisted form of the direct product:

$$\mathbb{Z}_n \rtimes U(n) = \{(x, a) \mid x \in \mathbb{Z}_n, a \in U(n)\}$$

with multiplication given by

$$(x, a)(y, b) = (x + ay, ab)$$

This has identity $(0, 1)$ and inverse $(x, a)^{-1} = (-a^{-1}x, a^{-1})$. Associativity is easy to check:

$$((x, a)(y, b))(x, c) = (x + ay + abz, abc) = (x, a)((y, b)(x, c))$$

If $n = 3$ then $U(3) \cong \mathbb{Z}_2$ and we get:

$$\mathbb{Z}_3 \rtimes \mathbb{Z}_2 \cong D_3 \cong S_3$$

(We know that there is only one nonabelian group of order $2p$.)

Since $U(n) \cong \text{Aut}(\mathbb{Z}_n)$, this construction is a special case of the semi-direct product:

$$G \rtimes \text{Aut}(G) = \{(x, \phi) \mid x \in G, \phi \in \text{Aut}(G)\}$$

with multiplication defined by

$$(x, \phi)(y, \psi) = (x\phi(y), \phi \circ \psi)$$

This semi-direct product is called the *holomorph* of G .