10. FINITELY GENERATED ABELIAN GROUPS

§10.1. Finitely Presented Abelian Groups

The group $\langle A, B, C \mid A^4 = B^2 = 1, AB = BA, AC = CA, BC = CB\rangle$ is an example of a finitely-presented abelian group, but one which is written multiplicatively. Additively we would write it as $\langle A, B, C \mid 4A = 2B = 0, A + B = B + A, A + C = C + A, B + C = C + B\rangle$. But if we're working entirely with abelian groups we know that the generators commute so we omit the commuting relations and use [ ] instead of $\langle\ \rangle$. We write the group simply as $[A, B, C \mid 4A = 2B = 0]$ or even more simply as $[A, B, C \mid 4A, 2B]$

We denote the abelian group generated by $X_1, \ldots, X_n$ subject to the relators $R_1, \ldots, R_m$ by $[X_1, \ldots, X_n \mid R_1, \ldots, R_m]$. (In the context of abelian groups the relators are written additively.)

Now a typical relator, R_i, can be written in the form $a_{i1}X_1 + \ldots + a_{in}X_n$ where the a_{ij} form an $m \times n$ matrix of integers A. Since the names of the generators are unimportant, and the number of them is the same as the number of columns of A, we can recover the presentation from just the integer matrix A.

For any $m \times n$ integer matrix $A = (a_{ij})$, [A] denotes the abelian group on n generators $X_1, \ldots, X_n$, subject to the m relations:

$$a_{11}X_1 + \ldots + a_{1n}X_n = 0$$
$$a_{21}X_1 + \ldots + a_{2n}X_n = 0$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_{m1}X_1 + \ldots + a_{mn}X_n = 0$$

Where the matrix is written in terms of its components we omit the usual matrix parentheses.

Example 1:

$\begin{bmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \\ 2 & 2 & 2 \end{bmatrix}$ denotes the abelian group: $[A, B, C \mid 8A = 8B = 8C = 0, 2A + 2B + 2C = 0]$.

Essentially a finitely-presented abelian group is a system of homogeneous linear equations, but with integer coefficients. The important difference between these and those that arise in linear algebra is that here, division is not permitted. For example an element, x, of order 8 satisfies $8x = 0$ which in linear algebra would imply that $x = 0$. But that's because in linear algebra the coefficients come from a field while for abelian groups they're integers. We can only divide by those integers that have integer iverses under multiplication, that is, ± 1.

Example 2: $\begin{bmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \end{bmatrix}$ denotes the abelian group $[X, Y, Z \mid 8X = 8Y = 8Z = 0]$.

This is clearly a direct sum of cyclic groups, each of order 8 and so the group is isomorphic to $\mathbf{Z}_8 \oplus \mathbf{Z}_8 \oplus \mathbf{Z}_8$.

Where the matrix is diagonal we can read off, from the diagonal elements, the nature of the corresponding abelian group as a direct sum of cyclic groups.

Example 3: $\begin{bmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ denotes the abelian group [X, Y, Z | 8X = 8Y = 0].

Strictly speaking we should have written down the third equation, 0Z = 0, but this is clearly redundant. The last generator has infinite order, so the group is isomorphic to $\mathbf{Z}_8 \oplus \mathbf{Z}_8 \oplus \mathbf{Z}$.

So where the diagonal entry is 0 the corresponding direct summand is $\mathbf{Z}$ (not $\mathbf{Z}_0$). In the above example the third row is superfluous so we can write:

$\begin{bmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 0 \end{bmatrix} \cong \begin{bmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \end{bmatrix} \cong \mathbf{Z}_8 \oplus \mathbf{Z}_8 \oplus \mathbf{Z}$.

§10.2. Elementary Row Operations

We're in a similar situation to that part of linear algebra that deals with the solution of systems of linear equations. Remember the powerful role played by the elementary row operations in the solution of such systems and the part they play in the Gaussian algorithm.

Let's review the three types of elementary row operations.

$R_i \leftrightarrow R_j$: swap rows i, j

This is equivalent to swapping a pair of equations in our system and, just as in linear algebra, this is permissible. The new system is equivalent to the original one and so the groups are isomorphic.

Example 4:

$\begin{bmatrix} 8 & 6 & 5 \\ 3 & 8 & -2 \\ 1 & 0 & -3 \end{bmatrix} \cong \begin{bmatrix} 3 & 8 & -2 \\ 8 & 6 & 5 \\ 1 & 0 & -3 \end{bmatrix}$ where we've swapped R_1 and R_2.

$R_i \div k$: Divide row i by k (k = ±1 only)

This is where our abelian group situation differs from the linear algebra one. Our "scalars" here are integers and division is not generally permitted. In fact the only values of k for which this operation is permissible are k = ±1.

$R_i - kR_j$: subtract k times row j from row i (k any integer)

This is the most useful of all the elementary row operations in linear algebra and so it is here. Of course in our context only integer values of k can be used here.

Example 5:

Let $G = \begin{bmatrix} 8 & 6 & 5 \\ 3 & 8 & -2 \\ 1 & 0 & -3 \end{bmatrix}$. Subtracting twice row 2 from row 1 we get $G \cong \begin{bmatrix} 2 & -10 & 9 \\ 3 & 8 & -2 \\ 1 & 0 & -3 \end{bmatrix}$.

Swapping rows 1 and 3 we get $G \cong \begin{bmatrix} 1 & 0 & -3 \\ 3 & 8 & -2 \\ 2 & -10 & 9 \end{bmatrix}$.

Now, mimicking the Gaussian algorithm we can subtract 3 times row 1 from row 2 and twice row 1 from row 3 to get 0's underneath the 1 in the first column.

$$G \cong \begin{bmatrix} 1 & 0 & -3 \\ 0 & 8 & 7 \\ 0 & -10 & 15 \end{bmatrix} \cong \begin{bmatrix} 1 & 0 & -3 \\ 0 & 8 & 7 \\ 0 & -2 & 22 \end{bmatrix} \cong \begin{bmatrix} 1 & 0 & -3 \\ 0 & 0 & 95 \\ 0 & -2 & 22 \end{bmatrix} \cong \begin{bmatrix} 1 & 0 & -3 \\ 0 & -2 & 22 \\ 0 & 0 & 95 \end{bmatrix} .$$

If we could reach a diagonal matrix we'd have identified the group as a direct sum of cyclic groups. But how do we get our 1 in the second column? Not by dividing. Not by subtracting rows. Perhaps we don't get a 1 there after all. This seems to be about as far as we can go. Any further elementary row operations would only make the matrix more complicated – less like a diagonal matrix. We need additional operations.

§10.3. Elementary Column Operations

Elementary row operations convert a set of homogeneous linear equations into an equivalent set for the same set of variables. Once we start using column operations we begin to change the variables. But if we're only interested in the structure of the group up to isomorphism we can use elementary column operations to produce a simpler set of equations on a different, but equivalent, generating set.

The simplest case would be that of swapping two columns. The effect is to swap the corresponding generators. The groups described by the presentations will be isomorphic.

Example 6: $\begin{bmatrix} 3 & 3 & 6 \\ 8 & 4 & 0 \\ 0 & 12 & 12 \end{bmatrix} = [a, b, c \mid 3a + 3b + 6c = 8a + 4b = 12b + 12c = 0]$

$$\cong [a, b, c \mid 3a + 3c + 6b = 0, 8a + 4c = 0, 12b + 12c = 0] \cong \begin{bmatrix} 3 & 6 & 3 \\ 8 & 0 & 4 \\ 0 & 12 & 12 \end{bmatrix}$$

The effect of swapping the two generators b and c is to swap two columns of the integer matrix of the presentation.

Equally simple is an operation of the form $C_j \times -1$ which changes the sign of every entry in a given column. If X_j is the corresponding generator this corresponds to replacing X_j by $-X_j$.

When it comes to subtracting an integer multiple of one column from another the effect on the generators is a little less obvious. Consider the following example:

Example 7:

$$\begin{bmatrix} 3 & 6 & 3 \\ 8 & 17 & 4 \\ 0 & 5 & 2 \end{bmatrix} = [X_1, X_2, X_3 \mid 3X_1 + 6X_2 + 3X_3 = 0, 8X_1 + 17X_2 + 4X_3 = 0, 5X_2 + 2X_3 = 0]$$

Define $X_1' = X_1 + 2X_2$. Clearly the group is generated by $\{X_1', X_2, X_3\}$ since $X_1 = X_1' - 2X_2$. Expressing the relations in terms of this new set of generators we get:

$3(X_1' - 2X_2) + 6X_2 + 3X_3 = 0, 8(X_1' - 2X_2) + 17X_2 + 4X_3 = 0, 5X_2 + 2X_3 = 0.$

So the group has the equivalent presentation

$[X_1', X_2, X_3 \mid 3X_1' + 3X_3 = 0, 8X_1' + X_2 + 4X_3 = 0, 5X_2 + 2X_3 = 0] \cong \begin{bmatrix} 3 & 0 & 3 \\ 8 & 1 & 4 \\ 0 & 5 & 2 \end{bmatrix}$. The effect of the change of variables $X_1 \to X_1' = X_1 + 2X_2$ is the elementary column operation $C_2 - 2C_1$. Note the change of sign and the swapping of the subscripts.

If the generators are $X_1, \ldots, X_n$:
$C_i \leftrightarrow C_j$ corresponds to $X_i \leftrightarrow X_j$
$C_i \times -1$ corresponds to $X_i \rightarrow -X_i$
$C_i - kC_j$ corresponds to $X_j \rightarrow X_j + kX_i$

Theorem 1: If the integer matrix B is obtained from A by a sequence of elementary row and column operations then [B] ≅ [A].

Example 8:

$$\begin{bmatrix}10&14&4\\12&16&8\\14&18&8\end{bmatrix} \cong \begin{bmatrix}4&14&10\\8&16&12\\8&18&14\end{bmatrix} \cong \begin{bmatrix}4&2&2\\8&-8&-4\\8&-6&-2\end{bmatrix} \cong \begin{bmatrix}4&2&2\\0&-12&-8\\0&-10&-6\end{bmatrix} \cong \begin{bmatrix}2&4&2\\-12&0&-8\\-10&0&-6\end{bmatrix} \cong \begin{bmatrix}2&0&0\\-12&24&4\\-10&20&4\end{bmatrix}$$

$C_1 \leftrightarrow C_3$; $C_2 - 3C_1, C_3 - 2C_1$; $R_2 - 2R_1, R_3 - 2R_1$; $C_1 \leftrightarrow C_2$; $C_2 - 2C_1, C_3 - C_1$

$$\cong \begin{bmatrix}2&0&0\\0&24&4\\0&20&4\end{bmatrix} \cong \begin{bmatrix}2&0&0\\0&4&24\\0&4&20\end{bmatrix} \cong \begin{bmatrix}2&0&0\\0&4&0\\0&4&-4\end{bmatrix} \cong \begin{bmatrix}2&0&0\\0&4&0\\0&0&-4\end{bmatrix} \cong \begin{bmatrix}2&0&0\\0&4&0\\0&0&4\end{bmatrix}$$

$R_2 + 6R_1, R_3 + 5R_1$; $C_2 \leftrightarrow C_3$; $C_3 - 6C_2$; $R_3 - R_2$; $R_3 \div -1$

We've managed to get the matrix of an equivalent presentation in diagonal form. But in terms of the new generators this is clearly a direct sum of cyclic groups, viz. $\mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_4$.

§10.4. The Fundamental Theorem of Finitely-Generated Abelian Groups

Using the elementary row and column operations we can convert every integer matrix to diagonal form, and hence we have the following theorem.

Theorem 2: Every finitely-presented abelian group is a direct sum of cyclic groups.
Proof: Let A be the presentation matrix for a finite presentation of an abelian group.
Case (1): A = (m) for some m:
We can multiply by –1, if necessary, so we may assume that $m \geq 0$.
Then $[A] \cong \mathbf{Z}$ if $m = 0$ and
$\mathbf{Z}_m$ if $m > 0$.
(Of course $\mathbf{Z}_1$ is the trivial group so may be removed if it arises.)

Case (2) A = (m , 0, ... , 0) for some m:
Clearly [A] is isomorphic to the direct sum of $\mathbf{Z}_m$ and the direct sum of $n - 1$ copies of $\mathbf{Z}$.

Case (3) A = $\begin{pmatrix}\mathbf{m}\\\mathbf{0}\\\mathbf{\ldots}\\\mathbf{0}\end{pmatrix}$ **for some m:** Clearly $[A] \cong \mathbf{Z}_m$.

Case (4) A is the m × n zero matrix:
Clearly [A] is isomorphic to the direct sum of n copies of **Z**.

Case (5) The general case:
Suppose now that $A \neq 0$ and has at least 2 rows and at least 2 columns. Choose a non-zero element with smallest absolute value. Permute rows and columns to bring it to the 1-1 position and, if necessary, multiply the first column by –1 to make it positive. Now subtract suitable multiples of the first row and column from the others so that all other entries in the first row and column are in the range $0 \leq x < a_{11}$. This whole process can be continued, reducing the smallest non-zero absolute value, until the matrix takes the form (m, 0, ... , 0), $\begin{pmatrix} m \\ 0 \\ ... \\ 0 \end{pmatrix}$ or $\begin{pmatrix} m & 0 \\ 0 & B \end{pmatrix}$ where m is a non-negative integer and B is an integer matrix with one less row and column.
The theorem now follows by induction on the number of generators.

Example 9:

$$\begin{bmatrix} 9 & 6 & 7 & 5 \\ 30 & 21 & 17 & 13 \\ 18 & 15 & 7 & 5 \end{bmatrix} \cong \begin{bmatrix} 5 & 9 & 6 & 7 \\ 13 & 30 & 21 & 17 \\ 5 & 18 & 15 & 7 \end{bmatrix} \cong \begin{bmatrix} 5 & 9 & 1 & 7 \\ 13 & 30 & 8 & 17 \\ 5 & 18 & 10 & 7 \end{bmatrix} \cong \begin{bmatrix} 1 & 5 & 9 & 7 \\ 8 & 13 & 30 & 17 \\ 10 & 5 & 18 & 7 \end{bmatrix} \cong \begin{bmatrix} 1 & 5 & 9 & 7 \\ 0 & -27 & -42 & -39 \\ 0 & -45 & -72 & -63 \end{bmatrix}$$

permute columns $C_3 - C_1$ permute columns $R_2 - 8R_1, R_3 - 10R_1$

$$\cong \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 27 & 42 & 39 \\ 0 & 45 & 72 & 63 \end{bmatrix} \cong \begin{bmatrix} 27 & 42 & 39 \\ 45 & 72 & 63 \end{bmatrix} \cong \begin{bmatrix} 27 & 42 & 12 \\ 45 & 72 & 18 \end{bmatrix} \cong \begin{bmatrix} 12 & 27 & 42 \\ 18 & 45 & 72 \end{bmatrix} \cong \begin{bmatrix} 12 & 3 & 42 \\ 18 & 9 & 72 \end{bmatrix} \cong \begin{bmatrix} 3 & 12 & 42 \\ 9 & 18 & 72 \end{bmatrix}$$

$C_5 - 5C_1, C_3 - 9C_1, C_4 - 7C_1$ omit $\mathbf{Z}_1$ $C_3 - C_1$ permute columns $C_2 - 2C_1$ permute columns

$$\cong \begin{bmatrix} 3 & 12 & 42 \\ 0 & -18 & -54 \end{bmatrix} \cong \begin{bmatrix} 3 & 0 & 0 \\ 0 & 18 & 54 \end{bmatrix} \cong \mathbf{Z}_3 \oplus [18 \;\; 54] \cong \mathbf{Z}_3 \oplus [18 \;\; 0] \cong \mathbf{Z}_3 \oplus \mathbf{Z}_{18} \oplus \mathbf{Z}$$

The above theorem deals with **finitely-presented** abelian groups, those where there's not only a finite set of generators, but where the relations that hold between them can be deduced from a finite set of relations. What about those that are merely finitely-generated?

By adapting the above argument slightly we can show that they too are direct sums of cyclic groups. And since direct sums of finitely many cyclic groups are finitely-presented it follows that all finitely-generated abelian groups are indeed finitely-presented!

Theorem 3: Every finitely-generated abelian group is a direct sum of cyclic groups.
Proof: Suppose we have a finitely-generated abelian group G. Consider the set of all relations that hold between the generators and let the coefficients be arranged in an integer array. This will in fact be a matrix with as many columns as there are generators, but with possibly infinitely many rows. Exactly the same algorithm can be used as before. With infinitely many rows of course there'd be practical difficulties in implementing it but since all the rows can be operated on in parallel there'd be no theoretical problem. The finiteness of the number of columns means that the algorithm will terminate eventually.

§10.5. Euler's Theorem

A ready source of finite abelian groups can be found as integers modulo m. Recall that if m is any positive integer $\mathbf{Z}_m^{\#}$ denotes the group of all numbers from 1 to m – 1 that are coprime with m, under the operation of multiplication modulo m. (The coprimeness ensures the existence of inverses.)

Example 10: $\mathbf{Z}_7^{\#} = \{1, 2, 3, 4, 5, 6\} \cong \mathbf{Z}_6$; $\mathbf{Z}_8^{\#} = \{1, 3, 5, 7\} \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2$;
$\mathbf{Z}_{10}^{\#} = \{1, 3, 7, 9\} \cong \mathbf{Z}_4$.

The order of $\mathbf{Z}_m^{\#}$ is denoted by φ(m). This function φ is called the **Euler φ function**. (NB you pronounce Euler as "Oiler".) It is an important function in number theory, with φ(m) being the number of numbers from 1 to m that are coprime with m.

Lemma: (Chinese Remainder Theorem)
If m, n are coprime then for all a, b ∈ **Z** there exists x ∈ **Z** such that:

$$x \equiv a \pmod m \text{ and}$$
$$x \equiv b \pmod n.$$

Proof: Since m, n are coprime there exist integers h, k such that $1 = mh + nk$.
Let $x = a + m(b - a)h$. Clearly $x \equiv a \pmod m$.
Now $x = a(1 - mh) + mhb$
$= nka + (1 - nk)b$
$= b + nk(a - b)$
$\equiv b \pmod n$.

Theorem 4: If m, n are coprime then $\mathbf{Z}_{mn}^{\#} \cong \mathbf{Z}_m^{\#} \times \mathbf{Z}_n^{\#}$.
(We use "×" here instead of "⊕" simply because we're using multiplicative notation.)
Proof: Suppose that m, n are coprime. Then $x \to (x, x)$ is a homomorphism from $\mathbf{Z}_{mn}^{\#}$ to $\mathbf{Z}_m^{\#} \otimes \mathbf{Z}_n^{\#}$ since x is coprime to mn if and only if it's coprime to both m and n. The kernel of this map is trivial since, if $x \to (1, 1)$, then $x - 1$ is a multiple of both m and n and so is a multiple of mn (because m and n are coprime). The fact that this map is onto is a consequence of the Chinese Remainder Theorem (the lemma above).

Corollary: If m, n are coprime $\varphi(mn) = \varphi(m)\,\varphi(n)$.

Theorem 5: If p is prime, $\varphi(p^n) = p^{n-1}(p - 1)$
Proof: Of the p^n numbers from 0 to $p^n - 1$ there are precisely p^{n-1} multiples of p. The remaining $p^n - p^{n-1} = p^{n-1}(p - 1)$ numbers will be precisely the ones with no factor in common with p^n. Hence $\varphi(p^n) = p^{n-1}(p - 1)$.

Example 11: $\varphi(200) = \varphi(2^3.5^2) = 2^2(2 - 1)\,5^1(5 - 1) = 4.1.5.4 = 80$.

Theorem 6: (Euler) If a is coprime with m then $a^{\varphi(m)} = 1 \pmod m$, or in other words, $a^{\varphi(m)}$ leaves a remainder of 1 when divided by m.
Proof: Suppose a is coprime with m. Then $a \in \mathbf{Z}_m^{\#}$. Suppose it has order n. By Lagrange's theorem n divides φ(m). Thus $\varphi(m) = nq$ for some $q \in \mathbf{Z}$. Now $a^{\varphi(m)} = (a^n)^q = 1^q = 1$.
Corollary: (Fermat) If p is prime then $a^p = a \pmod p$.
Proof: If p divides "a" then LHS = RHS = 0. Otherwise, by Euler's theorem $a^{p-1} \equiv 1 \pmod p$.

Euler's theorem can be used to calculate the remainders of certain very large numbers.

Example 12: What is the remainder on dividing 5^{1000} by 42?
Solution: $\varphi(42) = \varphi(2.3.7) = 12$ so $5^{12} = 1 \pmod{42}$. NB We note that 5 is coprime to 42.
Dividing 1000 by 12 we get a remainder of 4. [$1000 = 12 * 83 + 4$]
So $5^{1000} = (5^{12})^{83}.5^4 = 1^{83}.5^4 = 625 = 37$.
Hence 5^{1000} leaves a remainder of 37 when divided by 42.
NOTE: To work this out directly, by calculating 5^{1000} first, would need far more computing power than is normally available.

In the decomposition of a finitely-generated group as a direct sum of cyclic groups the only finite summands we need are those whose orders are prime powers. This is because of the following theorem, which parallels Theorem 5.

Theorem 7: If m, n are coprime then $\mathbf{Z_{mn} \cong Z_m \oplus Z_n}$.
Proof: Let $x = (1, 1) \in \mathbf{Z}_m \oplus \mathbf{Z}_n$. Then $kx = (k, k) = (0, 0)$ if and only if k is both a multiple of m and n. Since m, n are coprime this requires k to be a multiple of mn and so x has order mn, the same as the order of the group $\mathbf{Z}_m \oplus \mathbf{Z}_n$ itself. Hence $\mathbf{Z}_m \oplus \mathbf{Z}_n$ is cyclic.

Example 13: $\mathbf{Z}_{24} \cong \mathbf{Z}_3 \oplus \mathbf{Z}_8$. Note that we can't split $\mathbf{Z}_8$ into $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$ because $\mathbf{Z}_8$ has only one element of order 2 while $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$ has 7 such elements.

§10.6. Some Important Subgroups of an Abelian Group

For an abelian group G we define $\mathbf{nG} = \{ng \mid g \in G\}$. Clearly this is a subgroup of G since $n(x + y) = nx + ny$ etc.

Examples 14:
(1) If $G = \mathbf{Z}_4 \oplus \mathbf{Z}_8$, $2G = \{(0, 0), (0, 2), (0, 4), (0, 6), (2, 0), (2, 2), (2, 4), (2, 6)\} \cong \mathbf{Z}_2 \oplus \mathbf{Z}_4$ and $3G = G$.
(2) If $G = \mathbf{Z}_4 \oplus \mathbf{Z}_6$, $2G = \{(0, 0), (0, 2), (0, 4), (2, 0), (2, 2), (2, 4)\} \cong \mathbf{Z}_2 \oplus \mathbf{Z}_3$ and
$3G = \{(0, 0), (0, 3), (3, 0), (3, 3), (2, 0), (2, 3), (1, 0), (1, 3)\} \cong \mathbf{Z}_4 \oplus \mathbf{Z}_2$.

Theorem 8: If G, H are abelian groups $\mathbf{n(G \oplus H) \cong nG \oplus nH}$.
Proof: The map $n(x, y) = (nx, ny)$ is the required isomorphism.

Theorem 9: $\mathbf{mZ_n \cong Z_d}$ where $\mathbf{d = \dfrac{n}{GCD(m, n)}}$.
Proof: mZ_n is clearly cyclic, generated by m and $km = 0$ in Z_n if and only if $n/(m, n) \mid k$. Thus m has order $n/(m, n)$ and generates a cyclic group isomorphic to $Z_{n/(m, n)}$.

Example 15:
If $G = \mathbf{Z}_{30} \oplus \mathbf{Z}_{100}$, $2G \cong \mathbf{Z}_{15} \oplus \mathbf{Z}_{50}$, $3G \cong \mathbf{Z}_{10} \oplus \mathbf{Z}_{100}$, $6G \cong \mathbf{Z}_5 \oplus \mathbf{Z}_{50}$ and $28G \cong \mathbf{Z}_{15} \oplus \mathbf{Z}_{25}$.

Another useful subgroup, for each positive integer n, is $\mathbf{G[n]} = \{g \in G \mid ng = 0\}$. It consists of those elements of G whose order divides n and it's clearly a subgroup of G since $nx = 0$ and $nx = 0$ imply $n(x + y) = 0$, etc.

Examples 16:
(1) If $G = \mathbf{Z}_4 \oplus \mathbf{Z}_8$, $G[2] = \{(0, 0), (0, 4), (2, 0), (2, 4)\} \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2$ and $G[3] = 0$.
(2) If $G = \mathbf{Z}_4 \oplus \mathbf{Z}_6$, $G[2] = \{(0, 0), (0, 3), (2, 0), (2, 3)\} \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2$ and
$3G = \{(0, 0), (0, 2), (0, 4)\} \cong \mathbf{Z}_3$.

Theorem 10: If G, H are abelian groups $(G \oplus H)[n] = G[n] \oplus H[n]$.
Proof: This is because $k(x, y) = 0$ if and only if $kx = 0$ in G and $ky = 0$ in H.

Theorem 11: $\mathbf{Z}_n[m] \cong \mathbf{Z}_{GCD(m, n)}$.
Proof: Suppose $k \in \mathbf{Z}_n[m]$. Then $mk = 0$ in Z_n and so $n \mid mk$. Hence $n/(m , n) \mid k$. Thus $\mathbf{Z}_n[m]$ is a cyclic group generated by $n/(m, n)$ and so is isomorphic to $\mathbf{Z}_{GCD(m, n)}$.

Example 17:
If $G = \mathbf{Z}_{30} \oplus \mathbf{Z}_{100}$, $G[2] \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2$, $G[3] \cong \mathbf{Z}_3$, $G[6] \cong \mathbf{Z}_6 \oplus \mathbf{Z}_2$ and $G[28] \cong \mathbf{Z}_2 \oplus \mathbf{Z}_4$.

§10.7. The Order Profile of a Finite Abelian Group.

Once a finite group G has been written as a direct sum of cyclic groups the numbers of elements of each order can be easily determined. This is because we can easily identify the subgroups G[n] for each n and hence recover the order information. A table that lists the numbers of elements of each order is called the **order profile** of the group.

Since the order of G[n] is the number of elements whose order divides n, we can count the number of elements of order n as follows:

$$\textbf{\# elements of order n} = |G[n]| \; - \sum_{d|n,\, d<n} \#\textit{elements of order } d$$

Example 18: Find the order profile of $G = \mathbf{Z}_4 \oplus \mathbf{Z}_6 \oplus \mathbf{Z}_9$.
Solution: Since $36G = 0$ the order of each element divides 36.
We list the subgroups G[n] and their orders:

n	**1**	**2**	**3**	**4**	**6**	**9**	**12**	**18**	**36**
G[n]	1	$\mathbf{Z}_2 \oplus \mathbf{Z}_2$	$\mathbf{Z}_3 \oplus \mathbf{Z}_3$	$\mathbf{Z}_4 \oplus \mathbf{Z}_2$	$\mathbf{Z}_2 \oplus \mathbf{Z}_6 \oplus \mathbf{Z}_3$	$\mathbf{Z}_3 \oplus \mathbf{Z}_9$	$\mathbf{Z}_4 \oplus \mathbf{Z}_6 \oplus \mathbf{Z}_3$	$\mathbf{Z}_2 \oplus \mathbf{Z}_6 \oplus \mathbf{Z}_9$	G
|G[n]|	1	4	9	8	36	27	72	108	216

So the order profile is:

order	number	
1	1	
2	3	= 4 – 1
3	8	= 9 – 1
4	4	= 8 – 3 – 1
6	24	= 36 –8 – 3 – 1
9	18	= 27 – 8 – 1
12	32	= 72 – 24 – 4 – 8 – 3 – 1
18	54	= 108 – 18 – 24 – 8 – 3 – 1
36	72	= 216 – 54 – 32 – 18 – 24 – 4 – 8 – 3 – 1
TOTAL	216	

The above process can be reversed. For a finite abelian group, knowing the number of elements of each order is sufficient to identify the group, up to isomorphism. (This can't be done with non-abelian groups).

Example 19: An abelian group has order $216 = 8 \times 27$. It could be any one of the following nine possibilities:

$\mathbf{Z}_8 \oplus \mathbf{Z}_{27}$	$\mathbf{Z}_4 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_{27}$	$\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_{27}$
$\mathbf{Z}_8 \oplus \mathbf{Z}_9 \oplus \mathbf{Z}_3$	$\mathbf{Z}_4 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_9 \oplus \mathbf{Z}_3$	$\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_9 \oplus \mathbf{Z}_3$
$\mathbf{Z}_8 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3$	$\mathbf{Z}_4 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3$	$\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_3$

Suppose we're given its order profile:

order	**number**
1	1
2	3
3	8
4	4
6	24
9	18
12	32
18	54
36	72
TOTAL	216

Let G_2 be the sum of those summands of the form $\mathbf{Z}_{2^n}$ and let G_3 be the sum of those summands of the form $\mathbf{Z}_{3^n}$. Then $G \cong G_2 \oplus G_3$. It remains to identify G_2 and G_3.

Now G[2] consists of those elements whose order divides 2, that is, the elements of order 2 plus the identity. We can see from the table that this has order $4 = 2^2$. Thus G_2 has exactly two cyclic summands in its decomposition as a direct sum of cyclic groups.
Hence $G_2 \cong \mathbf{Z}_2 \oplus \mathbf{Z}_4$.

Similarly G[3] has order 9 and so G_3 must be $\mathbf{Z}_3 \oplus \mathbf{Z}_9$ giving $G \cong \mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_9$. Note that this is not in the form that we began with in the previous example, but since $\mathbf{Z}_2 \oplus \mathbf{Z}_3 \cong \mathbf{Z}_6$ it can be easily brought to that form if we desire.

If a Sylow p-subgroup has order p^4 and G[p] has order p^2 we know that it has two cyclic direct summands in its decomposition, but we don't know whether it is $\mathbf{Z}_{p^2} \oplus \mathbf{Z}_{p^2}$ or $\mathbf{Z}_p \oplus \mathbf{Z}_{p^3}$. In such a case we'd need to examine elements of higher order. In the first case $G[p^2]$ would have order p^4 while in the second case it would have order p^3.

Example 20: The order profile for an abelian group of order 64 is:

order	**number**
1	1
2	7
4	24
8	32
TOTAL	64

So G[2] has order $8 = 2^3$ so is isomorphic to $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$. Thus there are 3 cyclic summands in the direct sum decomposition.

Since G[4] has order $1 + 7 + 24 = 32 = 2^5$ it's isomorphic to $\mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_4$, so one of the cyclic summands is just $\mathbf{Z}_2$. Since G[8] has order $64 = 2^6$ it must be $\mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_8$. But clearly G[8] = G so $G \cong \mathbf{Z}_2 \oplus \mathbf{Z}_4 \oplus \mathbf{Z}_8$.

§10.8. The Alexander Group of a Knot

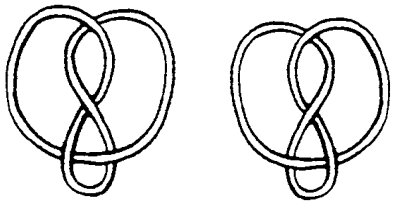
There are many places throughout mathematics where finitely-generated abelian groups arise in a very natural way. One of these is that part of topology that studies knots.

What motivates knot theorists is not the desire to come up with a better knot for tying things (even though the knots we tie in ropes, such as the granny knot, are indeed knots in the knot theorist's sense).

Last century chemists believed that space was knotted and that this was somehow connected to the chemical properties of a substance. This caused a flurry of activity in the area. Later it proved not to be the case and so for many decades knot theory was considered as a bit of a curiosity. But in the last twenty years there's been a resurgence of activity. This is partly because new methods were developed (and in the first instance by a physicist) and partly because physicists and biologists have begun to see knotted-ness in the things they study such as molecular flows and DNA.

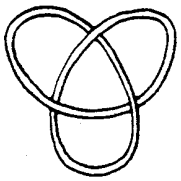
A **knot** is a closed curve in $\mathbf{R}^3$ that does not intersect itself. The knots we tie have two loose ends. But in order to keep the integrity of a knot, so that it doesn't change into another, we need to keep the ends far apart, or better still, we simply join them together.

Example 21: The figure 8 knot and its mirror image are:



Two knots are **equivalent** if one can be deformed into the other without breaking it open.

Example 22: The above figure 8 knots are equivalent. The proof is in the doing. Take a piece of string, tie the knot and then join the ends together. Manipulate the knot, without untying, so that it looks like the other picture.



But the figure 8 knot is not equivalent to the trefoil knot, shown at the right. This is not simply because of a different number of crossings. For example in the pictures of the figure 8 knot above, if we change the over/under nature of the top two crossings it becomes equivalent to the trefoil even though it would still have four crossings. (You can demonstrate this with an actual piece of string!)

To prove that two knots are inequivalent we need to construct an **invariant**, that is, a mathematical object that remains the same as a knot is manipulated.

The **Alexander group A(K)** of a knot is an abelian group that is just such an invariant. If two knots have non-isomorphic groups they're inequivalent (though if they have isomorphic Alexander groups they may still be inequivalent).

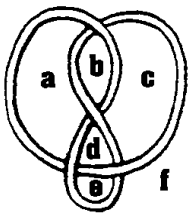
Suppose a knot has a projection with n crossings. Regarding this as a map on the sphere (the outside being counted as a region) there are n vertices and n edges. By Euler's theorem: $V + F - E = 2$ where $V = E = n$. There are thus $n + 2$ "faces" or regions. The generators of A(K) are these $n + 2$ regions. There are n relations, one for each crossing.

If the regions surrounding a crossing are a, b, c, d, with a, b one side of the overpass and c, d on the other

$$\begin{array}{c|c} a & b \\ \hline c & d \end{array}$$

the corresponding relation is a + b = c + d.

Example 23:
A(K) = [a, b, c, d, e, f | a + b = c + f, a + d = b + c, a + f = d + e, c + d = e + f]



$$\cong \begin{bmatrix} 1 & 1 & -1 & 0 & 0 & -1 \\ 1 & -1 & -1 & 1 & 0 & 0 \\ 1 & 0 & 0 & -1 & -1 & 1 \\ 0 & 0 & 1 & 1 & -1 & -1 \end{bmatrix} \cong \mathbf{Z} \oplus \mathbf{Z} \oplus \mathbf{Z}_5.$$

EXERCISES FOR CHAPTER 10

EXERCISE 1: For each of the following statements determine whether it is true or false.
(1) All cyclic groups are abelian.
(2) All abelian groups are cyclic.
(3) $\begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}$ is a cyclic group.
(4) $\begin{bmatrix} 2 & 0 & 2 \\ 0 & 2 & 2 \\ 0 & 0 & 0 \end{bmatrix} \cong \begin{bmatrix} 2 & 0 & 2 \\ 0 & 2 & 2 \end{bmatrix}$.
(5) $\begin{bmatrix} 2 & 2 & 0 \\ 0 & 8 & 0 \end{bmatrix} \cong \begin{bmatrix} 2 & 2 \\ 0 & 8 \end{bmatrix}$.
(6) $\mathbf{Z}_8 \oplus \mathbf{Z}_{10} \cong \mathbf{Z}_{80}$.
(7) $\mathbf{Z}_8 \oplus \mathbf{Z}_{11} \cong \mathbf{Z}_{88}$.
(8) Every finitely generated abelian group is a direct sum of cyclic groups of prime power order.
(9) $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$ has more elements of order 2 than $\mathbf{Z}_2 \oplus \mathbf{Z}_4$.
(10) Every non-trivial subgroup of $\mathbf{Z}$ is isomorphic to $\mathbf{Z}$.

EXERCISE 2: Write down the relation matrix for the abelian group:

[A, B, C | 8A = 2B, 8C = 4A, 10B + 12C = 0]

EXERCISE 3: Write down the relation matrix for the abelian group $\mathbf{Z}_{16} \oplus \mathbf{Z}_2 \oplus \mathbf{Z}$.

EXERCISE 4: Write Z_{3000} as a direct sum of cyclic groups of prime power order.

EXERCISE 5: Write the abelian group [A, B | 4A + 4B = 6A + 8B] as a direct sum of cyclic groups.

EXERCISE 6: Write the abelian group [A, B, C | 2A + 2B + 2C = 0] as a direct sum of cyclic groups.

EXERCISE 7: Write the following abelian group as a direct sum of cyclic groups of prime power order: $\begin{bmatrix} 11 & 22 & 13 \\ 14 & 25 & 16 \\ 19 & 50 & 23 \end{bmatrix}$.

SOLUTIONS FOR CHAPTER 10

EXERCISE 1:
(1) TRUE; (2) FALSE; (3) TRUE; (4) TRUE; (5) FALSE; (6) FALSE; (7) TRUE; (8) FALSE (infinite ones are not); (9) TRUE; (10) TRUE.

EXERCISE 2: $\begin{bmatrix} 8 & -2 & 0 \\ 4 & 0 & -8 \\ 0 & 10 & 12 \end{bmatrix}$.

EXERCISE 3: $\begin{bmatrix} 16 & 0 & 0 \\ 0 & 2 & 0 \end{bmatrix}$

EXERCISE 4: $\mathbf{Z}_{125} \oplus \mathbf{Z}_8 \oplus \mathbf{Z}_3$

EXERCISE 5: The relation matrix is $\begin{bmatrix} 4 & 4 \\ 6 & 8 \end{bmatrix} \cong \begin{bmatrix} 4 & 4 \\ 2 & 4 \end{bmatrix} \cong \begin{bmatrix} 2 & 4 \\ 4 & 4 \end{bmatrix} \cong \begin{bmatrix} 2 & 4 \\ 0 & -4 \end{bmatrix} \cong \begin{bmatrix} 2 & 0 \\ 0 & -4 \end{bmatrix} \cong \begin{bmatrix} 2 & 0 \\ 0 & 4 \end{bmatrix}$
$\cong \mathbf{Z}_2 \oplus \mathbf{Z}_4$.

EXERCISE 6: The groups is $[2, 2, 2] \cong [2, 0, 0] \cong \mathbf{Z}_2 \oplus \mathbf{Z} \oplus \mathbf{Z}$.

EXERCISE 7:
$\begin{bmatrix} 11 & 22 & 13 \\ 14 & 25 & 16 \\ 19 & 50 & 23 \end{bmatrix} \cong \begin{bmatrix} 11 & 22 & 13 \\ 3 & 3 & 3 \\ 8 & 28 & 10 \end{bmatrix} \cong \begin{bmatrix} 3 & 3 & 3 \\ 11 & 22 & 13 \\ 8 & 28 & 10 \end{bmatrix} \cong \begin{bmatrix} 3 & 3 & 3 \\ 2 & 13 & 4 \\ 2 & 22 & 4 \end{bmatrix} \cong \begin{bmatrix} 2 & 13 & 4 \\ 3 & 3 & 3 \\ 2 & 22 & 4 \end{bmatrix} \cong \begin{bmatrix} 2 & 13 & 4 \\ 1 & -10 & -1 \\ 0 & 9 & 0 \end{bmatrix}$
$\cong \begin{bmatrix} 1 & -10 & -1 \\ 2 & 13 & 4 \\ 0 & 9 & 0 \end{bmatrix} \cong \begin{bmatrix} 1 & -10 & -1 \\ 0 & 33 & 6 \\ 0 & 9 & 0 \end{bmatrix} \cong \begin{bmatrix} 1 & 0 & 0 \\ 0 & 33 & 6 \\ 0 & 9 & 0 \end{bmatrix} \cong \begin{bmatrix} 33 & 6 \\ 9 & 0 \end{bmatrix} \cong \begin{bmatrix} 9 & 0 \\ 33 & 6 \end{bmatrix} \cong \begin{bmatrix} 9 & 0 \\ 6 & 6 \end{bmatrix} \cong \begin{bmatrix} 6 & 6 \\ 9 & 0 \end{bmatrix} \cong \begin{bmatrix} 6 & 6 \\ 3 & -6 \end{bmatrix}$
$\cong \begin{bmatrix} 3 & -6 \\ 6 & 6 \end{bmatrix} \cong \begin{bmatrix} 3 & -6 \\ 0 & 18 \end{bmatrix} \cong \begin{bmatrix} 3 & 0 \\ 0 & 18 \end{bmatrix} \cong \mathbf{Z}_3 \oplus \mathbf{Z}_{18} \cong \mathbf{Z}_3 \oplus \mathbf{Z}_9 \oplus \mathbf{Z}_2$.