9. FINITELY GENERATED ABELIAN GROUPS

§9.1. Abelian Groups

An **abelian group** $(G, *)$ is a set G with a binary operation $*$ such that:

(1) (Closure Law) if $x, y \in G$ then $x * y \in G$;

(2) (Associative Law) $x * (y * z) = (x * y) * z$ for all $x, y, z \in G$;

(3) (Identity Law) there exists an element $e \in G$ such that $x * e = x$ for all $x \in G$;

(4) (Inverse Law) for all $x \in G$ there exists an element $y \in G$ such that $x * y = e$.

(5) (Commutative Law) $x * y = y * x$ for all $x, y \in G$.

These are called the axioms for abelian groups. They're not axioms in the sense that's often used in Euclidean geometry – as supposedly self-evident truths. Rather they're properties that a mathematical system, with one binary operation, might or might not

have. If a system satisfies all five properties then it qualifies as an abelian group.

A **binary operation** on G is simply a function f: $G \times G \to G$, that is, a function of two variables in G that assigns to every pair of elements $a, b \in G$ an element $f(a, b) \in G$. But it's more usual to write the name of the function between the two variables, so that instead of writing $*(a, b)$ we write $a * b$.

In other words we're talking about algebraic systems with a sort of abstract addition or multiplication, where we can combine any two elements. But the elements need not be numbers and the operation need not have any connection with ordinary arithmetic.

All that's required is some definition of a binary operation that satisfies all five of the above properties. Leaving out the last axiom we have the axioms for a **group**. The adjective 'abelian' qualifies the group structure by insisting that it satisfy the commutative law. [The word 'abelian' derives from the Norwegian mathematician Abel.]

Example 1: The most obvious examples of abelian groups are systems of numbers where addition is just ordinary addition.
$(\mathbb{R}, +)$ is the abelian group of real numbers under ordinary addition.

$(\mathbb{Q}, +)$ is the abelian group of rational numbers under ordinary addition.
$(\mathbb{Z}, +)$ is the abelian group of integers under ordinary addition.
$(2\mathbb{Z}, +)$ is the abelian group of even integers under ordinary addition.

Example 2: Sets of numbers can be abelian groups under multiplication. But we'd need to leave out zero because zero doesn't have an inverse under multiplication.
$(\mathbb{R}^{\#}, \times)$ is the abelian group of non-zero real numbers under multiplication.
$(\mathbb{Q}^{\#}, \times)$ is the abelian group of non-zero rational numbers under multiplication.

Example 3: Systems which *don't* qualify as abelian groups include:
The set of prime numbers under addition: This isn't an abelian group because it doesn't satisfy the closure law – the sum of two prime numbers isn't always a prime number.

The set of real numbers under subtraction: This isn't an abelian group because subtraction isn't associative. If it were we'd have to have $x - (y - z) = (x - y) - z$, which isn't the case.

The set of all 2×2 invertible real matrices, under matrix multiplication: This is a group, but not an abelian one – the commutative law doesn't hold.

The set of all positive real numbers under addition: This isn't an abelian group because there's no identity – zero, the identity for addition, isn't in this set.

The set of all positive integers, under multiplication: This isn't an abelian group because it doesn't contain inverses for all its elements: ½ isn't an integer, for example.

Example 4: Here's an abelian group where the set consists of numbers but where the operation is neither addition nor multiplication. Instead it's a combination of the two.

(G, $*$) where G is $\{x \in \mathbb{R} \mid x \neq -1\}$ and where $*$ is defined by $x * y = xy + x + y$.

Closure Law: Suppose $x, y \in$ G. We have to show that $xy + x + y \in$ G. Clearly it's a real number. All we have to do is to check that it can't be -1.
Suppose that $xy + x + y = -1$. Then $xy + x + y + 1 = 0$, so $(x + 1)(y + 1) = 0$.
Being real numbers we can conclude that $x + 1 = 0$ or $y + 1 = 0$, that is, $x = -1$ or $y = -1$.
But, being elements of G, neither is equal to -1.

Associative Law: Let $x, y, z \in G$. Then

$$x * (y * z) = x(y * z) + x + (y * z)$$
$$= x(yz + y + z) + x + (yz + y + z)$$
$$= xyz + xy + xz + x + yz + y + z$$

On the other hand $(x * y) * z$

$$= (x * y)z + x * y + z$$
$$= (xy + x + y)z + xy + x + y + z$$
$$= xyz + xz + yz + xy + x + y + z.$$

These are clearly equal.

Commutative Law: This is the only one of the five axioms that's immediately obvious.

Identity Law: $x * 0 = x0 + x + 0 = x$ for all $x \in G$ so 0 is the identity of this group. In other words $e = 0$ for this group.

Inverse Law: It's not nearly so obvious what should be the inverse of x so let's suppose that it's y. Then we'd have to have $xy + x + y = 0$, the identity.

Thus $y(x + 1) = -x$.

Now $x + 1$ is never zero if $x \in G$ so we may write

$$y = \frac{-x}{x + 1}.$$

Let's check: $x * \left(\frac{-x}{x + 1}\right) = x\left(\frac{-x}{x + 1}\right) + x + \left(\frac{-x}{x + 1}\right)$

$$= \frac{-x^2 + x(x + 1) - x}{x + 1} = 0.$$

All of the examples given so far have been infinite. We'll now give some finite examples.

The **order** of a finite abelian group is its size, that is, the number of elements that it contains. We denote the order of a finite abelian group G (or any finite group for that matter) by **|G|**.

Example 5: {1, –1, i, –i} is an abelian group of order 4 under multiplication.

Example 6: The following table defines a binary operation under which {*a*, *b*, *c*, *d*} is an abelian group.

*	***a***	***b***	***c***	***d***
a	*c*	*d*	*a*	*b*
b	*d*	*c*	*b*	*a*
c	*a*	*b*	*c*	*d*
d	*b*	*a*	*d*	*c*

Closure is obvious. The associative law is somewhat tedious to check, but this operation is indeed associative. Commutativity is obvious. The identity is clearly *c*. Finally, since *c* appears in every row and column every element has in inverse. In fact, in this example, *c* appears all the way down the diagonal, which means that every element of this group is its own inverse.

This is an abelian group of order 4, like the one in example 5. But they're quite different in structure. It's not just the different names for the elements. The group in example 6 satisfies the property that x^2 is the identity for all x. The group in example 5 doesn't. We'll formalise this later by saying that these two groups are not 'isomorphic' to one another.

Example 7: Let $G = \{0, 1, 2, 3, 4, 5, 6\}$ and let $x * y$ be the remainder on dividing $x + y$ by 7.

So $x * y = \begin{cases} x + y \text{ if } x + y < 7 \\ x + y - 7 \text{ if } x + y \geq 7 \end{cases}$

(G, $*$) is an abelian group and |G| = 7. This group is called the group of integers modulo 7 (or 'mod 7' for short). We denote it by $\mathbb{Z}_7$ and we usually use the symbol '+' instead of '$*$'. You just have to be careful to know whether you're talking about ordinary arithmetic or mod 7 arithmetic.

Although 3 + 5 = 8 in ordinary arithmetic it's 1 in mod 7 arithmetic. We can describe mod 7 arithmetic by a group table.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

This group may look strange, but remember that it's precisely the group you can use when calculating days of the week, where Monday = 0, Tuesday = 1 etc. If today is Friday (day 4) and something is happening 5 days later you can simply add 4 and 5 modulo 7 and get 2. So that event will be on a Wednesday.

Never mind that 4 + 5 = 9 in ordinary arithmetic. If we're only interested in days of the week then 7 days are equivalent to no days!

Example 8: The group table for $\mathbb{Z}_4$ is:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	1	2
3	3	0	1	2

This has the same pattern as the group in example 5. If you replace 1 by 0, i by 1, –1 by 2 and –i by 3 in that group, you'll get exactly the same operation as in this table.

More generally, for any positive integer n, we define the group of integers modulo n to be

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

under the operation of addition modulo n.

We denote this group by $\mathbb{Z}_n$ and, of course, $|\mathbb{Z}_n| = n$.

§9.2. Isomorphic Groups

We capture the idea of two groups having essentially the same structure by introducing the concept of *isomorphisms* and *isomorphic groups*.

We define an **isomorphism** between groups $(G, *)$ and $(H, \bullet)$ to be a 1-1 and onto function $f: G \to H$ such that $f(x * y) = f(x) \bullet f(y)$ for all $x, y \in G$. In the case of the function $f:\{1, i, -1, -i\} \to \mathbb{Z}_4$ we'd take $f(1) = 0$, $f(i) = 1$, $f(-1) = 2$ and $f(-i) = 3$.

Two groups are **isomorphic** if there's an isomorphism from one to the other. So $\{1, i, -1, -i\}$ under multiplication is isomorphic to $\mathbb{Z}_4$. If $(G, *)$ is isomorphic to $(H, \bullet)$ we write $(G, *) \cong (H, \bullet)$. Usually we drop the notation for the operations and simply write $\mathbf{G \cong H}$.

Isomorphism is an equivalence relation. This means that for all groups G, H, K:

- $G \cong G$;
- if $G \cong H$ then $H \cong G$;
- if $G \cong H$ and $H \cong K$ then $G \cong K$.

More informally we can say that two groups are isomorphic if the elements of one can be renamed as the elements of the other so that the operation is the same in both groups.

Example 9:
The following two groups, G, H are defined by means of group tables.

G	**0**	**1**	**2**	**3**	**4**	**5**
0	3	5	4	0	2	1
1	5	4	3	1	0	2
2	4	3	5	2	1	0
3	0	1	2	3	4	5
4	2	0	1	4	5	3
5	1	2	0	5	3	4

H	**a**	**b**	**c**	**d**	**e**	**f**
a	f	d	e	b	c	a
b	d	e	f	c	a	b
c	e	f	d	a	b	c
d	b	c	a	e	f	d
e	c	a	b	f	d	e
f	a	b	c	d	e	f

The following is an isomorphism from G to H:

x	0	1	2	3	4	5
θ(*x*)	*a*	*c*	*b*	*f*	*d*	*e*

To check this we translate the group table for G by means of this function:

θ(G)	***a***	***c***	***b***	***f***	***d***	***e***
a	*f*	*e*	*d*	*a*	*b*	*c*
c	*e*	*d*	*f*	*c*	*a*	*b*
b	*d*	*f*	*e*	*b*	*c*	*a*
f	*a*	*c*	*b*	*f*	*d*	*e*
d	*b*	*a*	*c*	*d*	*e*	*f*
e	*c*	*b*	*a*	*e*	*f*	*d*

Now we rearrange rows:

θ(G)	***a***	***c***	***b***	***f***	***d***	***e***
a	*f*	*e*	*d*	*a*	*b*	*c*
b	*d*	*f*	*e*	*b*	*c*	*a*
c	*e*	*d*	*f*	*c*	*a*	*b*
d	*b*	*a*	*c*	*d*	*e*	*f*
e	*c*	*b*	*a*	*e*	*f*	*d*
f	*a*	*c*	*b*	*f*	*d*	*e*

and finally we rearrange columns:

θG)	***a***	***b***	***c***	***d***	***e***	***f***
a	*f*	*d*	*e*	*b*	*c*	*a*
b	*d*	*e*	*f*	*c*	*a*	*b*
c	*e*	*f*	*d*	*a*	*b*	*c*
d	*b*	*c*	*a*	*e*	*f*	*d*
e	*c*	*a*	*b*	*f*	*d*	*e*
f	*a*	*b*	*c*	*d*	*e*	*f*

This is now identical to the group table for H.

§9.3. Direct Sums

If (G, $*$) and (H, $\bullet$) are abelian groups their **direct sum** is the group ($\mathbf{G} \oplus \mathbf{H}$, #) whose elements are the ordered pairs (g, h) for $g \in$ G and $h \in$ H and where:

$$(g_1, h_1) \# (g_2, h_2) = (g_1 * g_2, h_1 \bullet h_2).$$

Usually we use 'additive notation' for both groups and their direct sum. This means that we write all operations as +. So in G ⊕ H we have

$$(g_1, h_1) + (g_2, h_2) = (g_1 + g_2, h_1 + h_2).$$

Clearly if G, H are finite groups, with |G| = m and |H| = n then |G ⊕ H| = mn.

Example 10: $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is an abelian group of order 4. Its four elements are (0, 0), (0, 1), (1, 0) and (1, 1) and the direct sum operation can be described by the following group table.

$\mathbb{Z}_2 \oplus \mathbb{Z}_2$	**(0, 0)**	**(0, 1)**	**(1, 0)**	**(1, 1)**
(0, 0)	(0, 0)	(0, 1)	(1, 0)	(1, 1)
(0, 1)	(0, 1)	(0, 0)	(1, 1)	(1, 0)
(1, 0)	(1, 0)	(1, 1)	(0, 0)	(0, 1)
(1, 1)	(1, 1)	(1, 0)	(0, 1)	(0, 0)

Compare this with the group table given in example 6. That group, and this one, are isomorphic. Notice that $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_4$.

Example 11: $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6$

Remember that, when adding ordered pairs in $\mathbb{Z}_2 \oplus \mathbb{Z}_3$, you must add modulo 2 in the first component but modulo 3 in the second.

$\mathbb{Z}_2 \oplus \mathbb{Z}_3$	**(0, 0)**	**(0, 1)**	**(0, 2)**	**(1, 0)**	**(1, 1)**	**(1, 2)**
(0, 0)	(0, 0)	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)
(0, 1)	(0, 1)	(0, 2)	(0, 0)	(1, 1)	(1, 2)	(1, 0)
(0, 2)	(0, 2)	(0, 0)	(0, 1)	(1, 2)	(1, 0)	(1, 1)
(1, 0)	(1, 0)	(1, 1)	(1, 2)	(0, 0)	(0, 1)	(0, 2)
(1, 1)	(1, 1)	(1, 2)	(1, 0)	(0, 1)	(0, 2)	(0, 0)
(1, 2)	(1, 2)	(1, 0)	(1, 1)	(0, 2)	(0, 0)	(0, 1)

The following is an isomorphism from $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ to $\mathbb{Z}_6$

x	(0, 0)	(0, 1)	(0, 2)	(1, 0)	(1, 1)	(1, 2)
$\theta(x)$	0	4	2	3	1	5

§9.4. Subgroups

From now on, except in some specific examples, we'll use + as the symbol for the binary operation in an abelian group and we'll denote the identity by the symbol '0'. If g is an element of an abelian group its inverse under addition will be denoted by $-g$. We'll also define $g - h$ to be $g + (-h)$. This is the notation we use for groups of numbers under addition, but remember we're not assuming that the elements of our groups are numbers or that addition is the one we learnt many years ago.

Suppose G is an abelian group and $g \in G$. If n is a positive integer we define ng to be the sum of n copies of g. We define $0g = 0$ and if $n = -m$ where $m > 0$ we define $ng = m(-g)$.

So, for example, $3g = g + g + g$. If there exists a positive integer n such that $ng = 0$ then we say that g has **finite order**. The smallest positive n for which $ng = 0$ is called the **order** of g.

Example 12: The order of $2 \in \mathbb{Z}_6$ is 3 because, mod 6, $2 \neq 0$, $2 + 2 = 4 \neq 0$ but $2 + 2 + 2 = 0$.

A subset H of an abelian group G is called a **subgroup** of G (denoted by $\mathbf{H \leq G}$) if:

(Closure under addition) $h_1, h_2 \in$ H implies that $h_1 + h_2 \in$ H;
(Closure under identity) $0 \in$ H;
(Closure under inverses) $h \in$ H implies that $-h \in$ H.

These properties ensure that H is itself an abelian group under addition. (We don't need to stipulate associativity, because if addition is associative for all elements of G it will certainly apply within H.)

Suppose that G is an abelian group and $H \leq G$. If $g \in$ G we define the **coset containing *g*** to be

$$\boldsymbol{g} + \mathbf{H} = \{g + h \mid h \in \mathrm{H}\}.$$

The element g is called a **representative** of the coset.

Example 13: If $G = \mathbb{Z}_{12}$ and $H = \{0, 3, 6, 9\}$ then $H \leq G$. The cosets of H are $H = 0 + H = \{0, 3, 6, 9\}$, $1 + H = \{1, 4, 7, 10\}$ and $2 + H = \{2, 5, 8, 11\}$.

There are other possible representatives, but they lead to the same cosets. For example $5 + H = \{5, 8, 11, 2\}$, remembering that $5 + 9 = 2 \bmod 12$, and this is the same as $2 + H$.

Theorem 1: If G is an abelian group and $H \leq G$ then distinct cosets of H are disjoint.
(This means that if two cosets have one element in common they must be the same coset.)
Proof: Suppose $g \in a + H$ and $g \in b + H$.
Then $g = a + h_1 = b + h_2$ for some $h_1, h_2 \in H$.
Hence $b = a + (h_1 - h_2)$.
So for any $h \in H$ we have:
$b + h = a + (h_1 - h_2 + h) \in a + H$.
This shows that $b + H \subseteq a + H$.
Similarly $a + H \subseteq b + H$ and so the two cosets are equal.

Theorem 2 (Lagrange's Theorem): If G is a finite abelian group and $H \leq G$ then $|H|$ divides $|G|$.
Proof: Suppose there are m distinct cosets of H. Since every element of G belongs to exactly one coset and since they all have the same size as H, we have

$$|G| = m.|H|.$$

The set $\{ng \mid n \in \mathbb{Z}\}$ is called the **cyclic subgroup** generated by g and is denoted by $\langle g \rangle$. This is a subgroup of G since $mg + ng = (m + n)g$, $0 = 0g$ and $-(ng) = (-n)g$. If finite, the order of this cyclic subgroup is the same as the order of the element g. It clearly

follows from Theorem 2 that the order of every element of a finite group must divide the order of that group.

§9.5. Generators and Relations

In abstract algebra, of which the theory of abelian groups forms a small but important part, the most important features are the underlying patterns, not what the elements actually are.

One abstract way to define an abelian group is to provide a group table. We can use this to find the sum of any two elements without having to be bothered about what the elements really are. But this is clearly no good for infinite groups.

Another way to define abelian groups abstractly is to use **generators and relations**. Suppose $x_1, x_2, \ldots, x_n$ are n symbols, representing nothing in particular. We can consider 'formal linear combinations' of these x_i. These are abstract expressions of the form:

$$a_1x_1 + \ldots + a_nx_n$$

where the coefficients, a_i, are integers.

We don't ask what the x_i are, or what addition means. If we have to add x_1 to x_2 the answer is simply $x_1 + x_2$. But we can add two of these formal linear combinations in the obvious way:

$$(a_1x_1 + \ldots + a_nx_n) + (b_1x_1 + \ldots + b_nx_n)$$
$$= (a_1 + b_1)x_1 + \ldots + (a_n + b_n)x_n$$

and the answer is yet another formal linear combination.

So the set of all formal linear combinations of the x_i is closed under addition. The associative law clearly holds. The identity is the formal linear combination $0x_1 + \ldots + 0x_n$ and the inverse of the formal linear combination $a_1x_1 + \ldots + a_nx_n$ is the formal linear combination $(-a_1)x_1 + \ldots + (-a_n)x_n$.

We denote the group of all formal linear combinations of $x_1, \ldots, x_n$ by $[x_1, \ldots, x_n]$.

Example 14: $[x, y] = \{mx + ny \mid m, n \in \mathbb{Z}\}$.
In this group the sum of $3x + 2y$ and $5x + (-7)y$ is

$$8x + (-5)y.$$

Now a moment's thought will make it clear that $[x, y]$

$$\cong \mathbb{Z} \oplus \mathbb{Z}$$

under the isomorphism $f(mx + ny) = (m, n)$.
Similarly for more generators and more copies of $\mathbb{Z}$. So generators, on their own, give us nothing new. It's the relations that really make things interesting.

Suppose we have a finite set of these formal linear combinations and we put each of these to zero.

$$\left.\begin{array}{l} a_{11}x_1 + \ldots + a_{1n}x_n = 0 \\ a_{21}x_1 + \ldots + a_{2n}x_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = 0 \end{array}\right\}$$

As a consequence of these relations we have to identify many of the formal linear combinations in our group to one another.

Example 15: Suppose we have two generators and one relation $3x + 5y = 0$. Then we also have the relation $7x + 10y = 7x + 10y + (3x + 5y) = 10x + 15y$. But we can't conclude from $10x + 15y = 0$ that $2x + 3y = 0$. Addition and subtraction are possible, but not division. This is because we're working entirely with integers and division by 5 means multiplication by 1/5, which isn't an integer.

We can, from $3x + 5y = 0$, deduce that $3x = -5y$ and so we can replace every $3x$ in a formal linear combination by this multiple of y. This means that the elements of our abelian group can be split into three disjoint subsets:
$\{ny \mid \mathrm{n} \in \mathbb{Z}\}$, $\{x + ny \mid n \in \mathbb{Z}\}$ and $\{2x + ny \mid n \in \mathbb{Z}\}$.

If the coefficient of x is anything else we can replace $3x$ by $-5y$ many times to bring the coefficient of x to being one of the three values 0, 1 or 2. These subsets are disjoint because if $x + ny = 2x + my$ for some $m, n \in \mathbb{Z}$ we'd have $x + (n - m)y = 0$ which is a relation

that's not a consequence of the one given. We always assume that there are no further relations other than those that follow from the ones given.

If we have such a set of relations

$$R_1 = R_2 = \ldots = R_m = 0$$

we denote the abelian group that's generated by x_1, x_2, … , x_n subject to these relations by

$$\mathbf{[}x_1, \ldots x_n \mid R_1 = R_2 = \ldots = R_m = 0\mathbf{]}.$$

Example 16: Consider $[x \mid 7x = 0]$. A formal linear combination of one generator is simply a formal multiple. So the elements of this group have the form nx for $n \in \mathbb{Z}$.

But, because of the relation $7x = 0$, the distinct elements are $0, x, 2x, 3x, 4x, 5x$ and $6x$ and, for example $4x + 5x = 9x = 2x + 7x = 2x + 0 = 2x$. It's clear that this group is simply the group of integers mod 7 in disguise. In other words $[x \mid 7x = 0] \cong \mathbb{Z}_7$.

Example 17: $[x, y \mid 3x = 0, 5y = 0] \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5$.

$[x, y \mid 3x = 0, 5y = 0]$

$= \{0, y, 2y, 3y, 4y, x, x + y, x + 2y, x + 3y, x + 4y,$

$2x, 2x + y, 2x + 2y, 2x + 3y, 2x + 4y\}$.

The function $f(mx + ny) = (m, n)$ is an isomorphism onto $\mathbb{Z}_3 \oplus \mathbb{Z}_5$.

§9.6. Relation Matrices

Rather than manipulate relations it's easier to manipulate just their coefficients, as the rows of a matrix. If we have m relations in n variables the relation matrix is the $m \times n$ matrix whose rows are the coefficients of the successive relations.

Example 18: The set of relations:

$$\left.\begin{matrix} 3x + 4y - 5z \\ 7x + 9z \end{matrix}\right\}$$

can be coded as the 2×3 matrix $\begin{pmatrix} 3 & 4 & -5 \\ 7 & 0 & 9 \end{pmatrix}$.

We can use this notation to provide a convenient way of representing abelian groups that are given in terms of generators and relations. We simply write down the relation matrix and, to show that what we have in mind is the abelian group, and not just the matrix, we use square brackets instead of the usual parentheses.

If A is an $m \times n$ integer matrix, with a_{ij} being the entry in the i-j position, then [A] denotes the abelian group $[x_1, \ldots x_n \mid a_{11}x_1 + \ldots + a_{1n}x_n = 0, \ldots.,$

$$a_{m1}x_1 + \ldots + a_{mn}x_n = 0].$$

We can use any variable names. The above group is clearly isomorphic to:

$[y_1, \ldots y_n \mid a_{11}y_1 + \ldots + a_{1n}y_n = 0, \ldots.,$

$$a_{m1}y_1 + \ldots + a_{mn}y_n = 0].$$

Where we have three variables we generally use the symbols x, y and z.

Example 19: $\begin{bmatrix} 3 & 7 \\ 2 & 4 \end{bmatrix} = [x, y \mid 3x + 7y = 2x + 4y = 0]$

Example 20: $\begin{bmatrix} 3 & 7 \\ 2 & 4 \end{bmatrix} = \begin{bmatrix} 2 & 4 \\ 3 & 7 \end{bmatrix}$. Here we've swapped the two rows, which means that we've simply swapped the relations.

Example 21: $\begin{bmatrix} 3 & 7 \\ 2 & 4 \end{bmatrix} \cong \begin{bmatrix} 7 & 3 \\ 4 & 2 \end{bmatrix}$. Here we've swapped the two columns. Strictly speaking these groups aren't equal, because in one group $3x + 7y = 0$ while in the other we have $3y + 7x = 0$. But the only difference is a swapping of the variables. This gives us a group that's isomorphic to the one we began with.

$\begin{bmatrix} 3 & 7 \\ 2 & 4 \end{bmatrix} = [x, y \mid 3x + 7y = 0, 2x + 4y = 0]$

$\cong [x, y \mid 7x + 3y = 0, 4x + 2y = 0] = \begin{bmatrix} 7 & 3 \\ 4 & 2 \end{bmatrix}$.

The isomorphism here is $f(ax + by) = bx + ay$.

So we can rearrange rows of a relation matrix without changing the corresponding abelian group and, if we rearrange the columns, we get a different group but one that's isomorphic to the original one. Since we're treating isomorphic groups as if they were the

same (they have the same structural pattern) we haven't changed the group under either of these operations.

Example 22: $\begin{bmatrix} 3 & 7 \\ 2 & 4 \end{bmatrix} = \begin{bmatrix} 23 & 47 \\ 2 & 4 \end{bmatrix}$. Here we've added 10 times row 2 to row 1. This has the effect of replacing the equation $3x + 7y = 0$ by $3x + 7y + 10(2x + 4y) = 23x + 47y = 0$. The new equation is a consequence of the original two. Furthermore if we have the two equations:

$$\left.\begin{matrix} 23x + 47y = 0 \\ 2x + 4y = 0 \end{matrix}\right\}$$

we can deduce the equation $3x + 7y = 0$ by subtracting 10 times the second equation from the first.

So the two sets of equations $\left.\begin{matrix} 3x + 7y = 0 \\ 2x + 4y = 0 \end{matrix}\right\}$ and $\left.\begin{matrix} 23x + 47y = 0 \\ 2x + 4y = 0 \end{matrix}\right\}$ are equivalent (they have the same consequences) and so the abelian groups $\begin{bmatrix} 3 & 7 \\ 2 & 4 \end{bmatrix}$ and $\begin{bmatrix} 23 & 47 \\ 2 & 4 \end{bmatrix}$ are identical.

Example 23: $\begin{bmatrix} 3 & 7 \\ 2 & 4 \end{bmatrix} \cong \begin{bmatrix} 73 & 7 \\ 42 & 2 \end{bmatrix}$. Here we've added 10 times the second column to the first. This new group is different to the first, but it's isomorphic to it. Let's see why.

$\begin{bmatrix} 3 & 7 \\ 2 & 4 \end{bmatrix} = [x, y \mid 3x + 7y = 0, 2x + 4y = 0]$.

Now let $z = y - 10x$. This means that $y = z + 10x$, so any formal linear combination in x and y can be expressed in terms of x and z.
For example $5x + 7y = 5x + 7(z + 10x) = 75x + 7z$. Hence x and z are equally good generators as x and y. But the relations translate into different relations when we express them in terms of x and z.

The system of equations $\left.\begin{matrix} 3x + 7y = 0 \\ 2x + 4y = 0 \end{matrix}\right\}$ when expressed in terms of x and z become:

$$\text{that is, } \left.\begin{matrix} 73x + 7z = 0 \\ 42x + 4z = 0 \end{matrix}\right\}.$$

$$\begin{aligned} \text{Hence } \begin{bmatrix} 3 & 7 \\ 2 & 4 \end{bmatrix} &\cong [x, y \mid 3x + 7y = 0,\ 2x + 4y = 0] \\ &\cong [x, z \mid 73x + 7z = 0,\ 42x + 4z = 0] \\ &\cong [x, y \mid 73x + 7y = 0,\ 42x + 4y = 0] \\ &\cong \begin{bmatrix} 23 & 47 \\ 2 & 4 \end{bmatrix}. \end{aligned}$$

Example 24: Let's see if we can simplify $\begin{bmatrix} 3 & 7 \\ 2 & 4 \end{bmatrix}$.

$$\begin{aligned} \begin{bmatrix} 3 & 7 \\ 2 & 4 \end{bmatrix} &\cong [x, y \mid 3x + 7y = 0,\ 2x + 4y = 0] \\ &\cong [x, y \mid (3x + 7y) - (2x + 4y) = 0,\ 2x + 4y = 0] \\ &\cong [x, y \mid x + 3y = 0,\ 2x + 4y = 0] \\ &\cong [x, y \mid x + 3y = 0,\ 2(x + 2y) = 0]. \end{aligned}$$

Let $z = x + 2y$. Then $[x, y \mid x + 3y = 0,\ 2(x + 2y) = 0]$

$$\cong [y, z \mid (z - 2y) + 3y = 0,\ 2z = 0]$$

$$\cong [y, z \mid y + z = 0, 2z = 0].$$

Now the relation $y + z = 0$ allows us to write $y = -z$. So any formal linear combination that can be expressed in terms of y and z can be expressed in terms of z alone. So we can drop y as a generator and remove the relation $y + z = 0$. Hence $[y, z \mid y + z = 0, 2z = 0]$

$$\cong [z \mid 2z = 0] \cong \mathbb{Z}_2.$$

All of these steps can be done purely in terms of the relation matrix by making suitable row and column operations. We'll now repeat it, just using matrices:

$$\begin{bmatrix} 3 & 7 \\ 2 & 4 \end{bmatrix} \cong \begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix} \cong \begin{bmatrix} 1 & 1 \\ 2 & 0 \end{bmatrix} \cong \begin{bmatrix} 0 & 1 \\ 2 & 0 \end{bmatrix} \cong \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$$

$$R_1 - R_2 \qquad C_2 - 2C_1 \qquad C_1 - C_2 \qquad C_1 \leftrightarrow C_2$$

$$\cong [2] \cong \mathbb{Z}_2.$$

Example 25: By similar methods we can show that $\begin{bmatrix} 3 & 7 \\ 1 & 2 \end{bmatrix}$ is the trivial group, consisting just of the identity. We denote this group by the symbol **0**. It's clear that this isn't isomorphic to the group $\begin{bmatrix} 3 & 7 \\ 2 & 4 \end{bmatrix}$ in example 24. This illustrates the fact that we're not permitted to divide the second row by 2.

So we represent an abelian group, given in terms of finitely many generators and relations, by an integer matrix and we use elementary row and column

operations to simplify it. These operations are very much like the elementary row and column operations from linear algebra, except that we don't allow multiplication or division by a constant (though multiplication by −1 is permitted).

Elementary integer row operations:

(1) $R_i \leftrightarrow R_j$: Swap rows i and j.

(2) $R_i \rightarrow -R_i$: Change the sign of row i.

(3) $R_i - kR_j$: Subtract k times row j from row i (where k is any integer).

Elementary integer column operations:

(1) $C_i \leftrightarrow C_j$: Swap columns i and j.

(2) $C_i \rightarrow -C_i$: Change the sign of column i.

(3) $C_i - kC_j$: Subtract k times column j from column i (where k is any integer).

Theorem 3: If a matrix B is obtained from a matrix A by a sequence of elementary row and column operations then [A] ≅ [B].

Proof: Let $G = [x_1, \ldots x_n \mid R_1 = \ldots = R_m = 0]$ where

$$R_i = a_{i1}x_1 + \ldots + a_{in}x_n$$

and let $A = (a_{ij})$ be the matrix of coefficients.

It's clear that the elementary row operations don't change the group. All they do is to change one set of relations into an equivalent set of relations. The

column operations are a little more difficult to see, since we need to change the generators.

$C_i \leftrightarrow C_j$ has the effect of swapping the generators x_i and x_j.

$C_i \to -C_i$ has the effect of replacing x_i by $-x_i$.

$C_i - kC_j$ is equivalent to replacing x_j by $x_j + kx_i$.
This one is a little more difficult to see. Suppose we define new generators $y_1, \ldots, y_n$ by:
$y_i = x_i$ if $i \neq j$;
$y_j = x_j + kx_i$.
It's clear that these new generators $y_1, \ldots y_n$ will generate the group, because we can express the old generators in terms of the new ones:
$x_i = y_i$ if $i \neq j$;
$x_j = y_j - kx_i = y_j - ky_i$ (remember that $i \neq j$ so $x_i = y_i$).

Now suppose that $a_1x_1 + \ldots + a_nx_n = 0$ is a relation between the old generators.
We can write this as:
$a_1x_1 + \ldots + (a_i - ka_j)x_i + \ldots + a_j(x_j + kx_i) + \ldots + a_nx_n = 0$.
[Here the omitted terms all have the form a_rx_r.]

Expressing this in terms of the new generators it becomes:

$a_1y_1 + \ldots + (a_i - ka_j)y_i + \ldots a_ix_j + \ldots a_nx_n = 0.$

Expressing all the relations in terms of these new generators the coefficient matrix has k times column j subtracted from column i.

§9.7. Direct Sums of Cyclic Groups

An abelian group G is **cyclic** if it can be generated by a single element, g. If g has order n then $G \cong \mathbb{Z}_n$. If g has infinite order then $G \cong \mathbb{Z}$. In the special case where g has order 1, g is itself the identity and so $G = \{0\}$. We denote the group of order 1 by the symbol **0**.

So the complete list of cyclic groups is:

0, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$,…… and $\mathbb{Z}$.

Moreover, no two of these cyclic groups are isomorphic since they all have different orders.

So if we have two cyclic groups and we find that they're isomorphic to different groups in this list then we know that they can't possibly be isomorphic to one another.

A matrix $A = (a_{ij})$ is a **diagonal matrix** if $a_{ij} = 0$ whenever $i \neq j$. So any non-zero entries lie on the (top-left to bottom-right) diagonal. Normally we reserve the term 'diagonal matrix' for a square matrix, but not here.

Example 26: $\begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 7 \\ 0 & 0 & 0 \end{pmatrix}$ is a diagonal matrix.

So is $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 7 & 0 \end{pmatrix}$.

If a relation matrix A is diagonal the abelian group [A] is a direct sum of cyclic groups.

Example 27: $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 8 \end{bmatrix} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_8.$

If there are more rows than columns in a diagonal matrix we must have one or more rows of zeros at the bottom. We can simply remove these rows: they represent the redundant relation 0 = 0.

Example 28: $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 8 \\ 0 & 0 & 0 \end{bmatrix} \cong \begin{bmatrix} 2 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 8 \end{bmatrix} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_8.$

If there are more columns than rows in a diagonal matrix we must have one or more columns of zeros at the right-hand end. Each one represents a variable that enters into no relation and contributes a

summand of $\mathbb{Z}$ to the direct sum of cyclic groups decomposition.

Example 29: $\begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 & 0 \\ 0 & 0 & 8 & 0 & 0 \end{bmatrix} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_8 \oplus \mathbb{Z} \oplus \mathbb{Z}.$

If there's a 1 on the diagonal of a diagonal matrix it represents a variable that is equated to zero. We can clearly ignore it, removing the row and column in which it lies.

Example 30: $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 8 \end{bmatrix} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_8.$

A **finitely generated abelian group** is one that has a finite set of generators. That is, where there's a finite set $\{x_1, x_2, \ldots, x_n\}$ such that every element of the group can be written as an integral linear combination $a_1x_1 + \ldots + a_nx_n$ for some $a_1, \ldots, a_n \in \mathbb{Z}$.

A concrete example of a finitely generated abelian group is any direct sum of finitely many cyclic groups. The **Fundamental Theorem of Abelian Groups** states that, up to isomorphism, this is all there is. In other words every finitely generated abelian group is isomorphic to one of the form:

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_r} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$$

where the number of copies of $\mathbb{Z}$ is finite (possibly zero).
In particular every *finite* abelian group is isomorphic to one of the form: $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_r}$.

Theorem 4: Every finitely generated abelian group is a direct sum of cyclic groups.
Proof: Suppose first that G is given by generators and relations as $[x_1, \ldots, x_n \mid R_1 = \ldots = R_m = 0]$. We can represent G by the $m \times n$ matrix of integer coefficients $A = (a_{ij})$. I'll show that any integer matrix can be converted to a diagonal matrix by a suitable sequence of elementary integer row and column operations.

(1) If there's a non-zero entry in the matrix choose one with the smallest absolute value and move it to the top-left-hand corner by suitable row and column swaps. (If the matrix is completely zero, we've finished.)

Example 31:
$$\begin{bmatrix} 5 & 8 & 7 \\ 8 & 10 & -9 \\ -5 & 6 & -4 \end{bmatrix} \cong \begin{bmatrix} 7 & 8 & 5 \\ -9 & 10 & 8 \\ -4 & 6 & -5 \end{bmatrix}$$
$$C_1 \leftrightarrow C_3$$
$$\cong \begin{bmatrix} -4 & 6 & -5 \\ -9 & 10 & 8 \\ 7 & 8 & 5 \end{bmatrix}.$$
$$R_1 \leftrightarrow R_3$$

(2) If the top-left-hand corner is negative make it positive by changing the sign of the top row.

Example 32: $\begin{bmatrix} -4 & 6 & -5 \\ -9 & 10 & 8 \\ 7 & 8 & 5 \end{bmatrix} \cong \begin{bmatrix} 4 & -6 & 5 \\ -9 & 10 & 8 \\ 7 & 8 & 5 \end{bmatrix}$.

$R_1 \to -R_1$

(3) Subtract suitable multiples of the first row from the remaining rows so that the entries in the first column, from row 2 down, are in the range $\{0, 1, 2, \ldots, m-1\}$. If any of these are positive we continue the process from step (1). The fact that the top-left corner entry is decreasing each time means that this process must eventually terminate.

Example 33: $\begin{bmatrix} 4 & -6 & 5 \\ -9 & 10 & 8 \\ 7 & 8 & 5 \end{bmatrix} \cong \begin{bmatrix} 4 & -6 & 5 \\ 3 & -8 & 23 \\ 3 & 14 & 0 \end{bmatrix}$

$R_2 + 3R_1, R_3 - R_1$

$\cong \begin{bmatrix} 3 & -8 & 23 \\ 4 & -6 & 5 \\ 3 & 14 & 0 \end{bmatrix}$.

$R_1 \leftrightarrow R_2$

(4) Once the first column has the form $\begin{pmatrix} m \\ 0 \\ \dots \\ 0 \end{pmatrix}$ we subtract suitable multiples of the first column from the remaining ones so that the entries in the first row, from the second column on, are in the range

$$\{0, 1, 2, \dots, m-1\}.$$

If any of these are positive we continue the process from step (1). Again, the fact that the top-left corner entry is decreasing each time means that this process must eventually terminate.

Example 34: $\begin{bmatrix} 3 & 7 & -9 \\ 0 & 6 & 4 \\ 0 & 4 & 5 \end{bmatrix} \cong \begin{bmatrix} 3 & 0 & 0 \\ 0 & 6 & 4 \\ 0 & 4 & 5 \end{bmatrix}$.

$C_2 - 7C_1, C_3 + 9C_1$

(5) Eventually we arrive at a matrix where the first column has the form $\begin{pmatrix} m \\ 0 \\ \dots \\ 0 \end{pmatrix}$ and the first row has the form $(m, 0, \dots, 0)$. We now have a direct summand of $\mathbb{Z}_m$ (ignore it if $m = 1$) and we can remove the first row and column to produce a smaller matrix. We then begin anew on this smaller matrix.

Example 35: $\begin{bmatrix} 3 & 0 & 0 \\ 0 & 6 & 4 \\ 0 & 4 & 5 \end{bmatrix} \cong \mathbb{Z}_3 \oplus \begin{bmatrix} 6 & 4 \\ 4 & 5 \end{bmatrix}$.

Example 36: $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 6 & 4 \\ 0 & 4 & 5 \end{bmatrix} \cong \begin{bmatrix} 6 & 4 \\ 4 & 5 \end{bmatrix}$.

(6) If the matrix is square we finally get a 1×1 matrix of the form (m) and so our final summand is:

$$\begin{cases} \mathbb{Z}_m \text{ if } m > 1 \\ \text{nothing if } m = 1 \\ \mathbb{Z} \text{ if } m = 0 \end{cases}$$

Example 37: $[5] \cong \mathbb{Z}_5$, $[1] \cong 0$, $[0] \cong \mathbb{Z}$.

If the matrix has more columns than rows we'll eventually get an $n \times 1$ matrix $\begin{pmatrix} m \\ 0 \\ \dots \\ 0 \end{pmatrix}$ where $n > 1$.

This gives us just $\mathbb{Z}_m$, nothing or $\mathbb{Z}$, depending on m as above. The 0's are redundant.

Example 38: $\begin{bmatrix} 7 \\ 0 \\ \dots \\ 0 \end{bmatrix} \cong [7] \cong \mathbb{Z}_7$.

If the matrix has more rows than columns we'll eventually get a $1 \times n$ matrix where $n > 1$. This will have the form $(m, 0, \ldots 0)$. This gives us $\mathbb{Z}_m$, nothing or $\mathbb{Z}$, as above, plus $n - 1$ copies of $\mathbb{Z}$.

Example 39: $[2, 0, 0, 0] \cong \mathbb{Z}_2 \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$.

In the general case, suppose that G is generated by $x_1, x_2, \ldots, x_n$. Let S be the set of all formal linear combinations that evaluate to 0 in G. This set will be but we could list them in some way and put the coefficients into a matrix with n columns and infinitely many rows. (If you've heard of the concepts of *countably infinite* and *uncountable* the set S is countably infinite.) The above proof will still be valid for such an infinite matrix.

Example 40:

$[x, y, z \mid 4x - y + 5z = 0, 14x + 7y + 7z = 0]$

$$\cong \begin{bmatrix} 4 & -1 & 5 \\ 14 & 7 & 7 \end{bmatrix} \cong \begin{bmatrix} -1 & 4 & 5 \\ 7 & 14 & 7 \end{bmatrix} \cong \begin{bmatrix} 1 & -4 & -5 \\ 7 & 14 & 7 \end{bmatrix}$$

$$\qquad\qquad C_1 \leftrightarrow C_2 \qquad\qquad R_1 \times (-1)$$

$$\cong \begin{bmatrix} 1 & -4 & -5 \\ 0 & 42 & 42 \end{bmatrix} \cong \begin{bmatrix} 1 & 0 & 0 \\ 0 & 42 & 42 \end{bmatrix} \cong \begin{bmatrix} 1 & 0 & 0 \\ 0 & 42 & 0 \end{bmatrix} \cong \mathbb{Z}_{42} \oplus \mathbb{Z}.$$

$R_2 - 7R_1 \qquad C_2 + 4C_1, C_3 + 5C_1$ etc.

Example 41:

$$\begin{bmatrix} 8 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \\ 2 & 2 & 2 \end{bmatrix} \cong \begin{bmatrix} 2 & 2 & 2 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \\ 8 & 0 & 0 \end{bmatrix} \cong \begin{bmatrix} 2 & 2 & 2 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \\ 0 & -8 & -8 \end{bmatrix}$$

$$\cong \begin{bmatrix} 2 & 0 & 0 \\ 0 & 8 & 0 \\ 0 & 0 & 8 \\ 0 & -8 & -8 \end{bmatrix}$$

$$\cong \mathbb{Z}_2 \oplus \begin{bmatrix} 8 & 0 \\ 0 & 8 \\ -8 & -8 \end{bmatrix} \cong \mathbb{Z}_2 \oplus \begin{bmatrix} 8 & 0 \\ 0 & 8 \\ 0 & -8 \end{bmatrix}$$

$$\cong \mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \begin{bmatrix} 8 \\ -8 \end{bmatrix}$$

$$\cong \mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \begin{bmatrix} 8 \\ 0 \end{bmatrix}$$

$$\cong \mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_8.$$

Example 42:

$$\begin{bmatrix} 3 & 7 & 5 & 9 \\ 7 & 2 & 4 & 6 \\ 3 & 2 & 7 & 2 \\ 2 & 3 & 4 & 5 \end{bmatrix} \cong \begin{bmatrix} 2 & 3 & 4 & 5 \\ 3 & 7 & 5 & 9 \\ 7 & 2 & 4 & 6 \\ 3 & 2 & 7 & 2 \end{bmatrix} \cong \begin{bmatrix} 2 & 3 & 4 & 5 \\ 1 & 4 & 1 & 4 \\ 1 & -7 & -8 & -9 \\ 1 & -1 & 5 & -3 \end{bmatrix}$$

$$\cong \begin{bmatrix} 1 & 4 & 1 & 4 \\ 2 & 3 & 4 & 5 \\ 1 & -7 & -8 & -9 \\ 1 & -1 & 5 & -3 \end{bmatrix} \cong \begin{bmatrix} 1 & 4 & 1 & 4 \\ 0 & -5 & 2 & -3 \\ 0 & -11 & -9 & -13 \\ 0 & -5 & 4 & -7 \end{bmatrix}$$

$$\cong \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -5 & 2 & -3 \\ 0 & -11 & -9 & -13 \\ 0 & -5 & 4 & -7 \end{bmatrix} \cong \begin{bmatrix} -5 & 2 & -3 \\ -11 & -9 & -13 \\ -5 & 4 & -7 \end{bmatrix}$$

$$\cong \begin{bmatrix} 2 & -5 & -3 \\ -9 & -11 & -13 \\ 4 & -5 & -7 \end{bmatrix} \cong \begin{bmatrix} 2 & -5 & -3 \\ 1 & -66 & -78 \\ 0 & 5 & -1 \end{bmatrix} \cong \begin{bmatrix} 1 & -66 & -78 \\ 2 & -5 & -3 \\ 0 & 5 & -1 \end{bmatrix}$$

$$\cong \begin{bmatrix} 1 & -66 & -78 \\ 0 & 125 & 153 \\ 0 & 5 & -1 \end{bmatrix} \cong \begin{bmatrix} 1 & 0 & 0 \\ 0 & 125 & 153 \\ 0 & 5 & -1 \end{bmatrix} \cong \begin{bmatrix} 125 & 153 \\ 5 & -1 \end{bmatrix}$$

$$\cong \begin{bmatrix} 5 & -1 \\ 125 & 153 \end{bmatrix} \cong \begin{bmatrix} -1 & 5 \\ 153 & 125 \end{bmatrix} \cong \begin{bmatrix} 1 & -5 \\ 153 & 125 \end{bmatrix}$$

$$\cong \begin{bmatrix} 1 & -5 \\ 0 & 890 \end{bmatrix} \cong \begin{bmatrix} 1 & 0 \\ 0 & 890 \end{bmatrix} \cong [890] \cong \mathbb{Z}_{890}.$$

§9.8. The Isomorphism Problem

There remains the problem of deciding when two direct sums of cyclic groups are isomorphic. For a start we can rearrange the summands and the group, up to isomorphism, doesn't change.

Example 43: $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2$.

But there are other ways in which different expressions of sums of cyclic groups can represent isomorphic groups.

Example 44: $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6$.
Let $g = (1, 1)$. The cyclic subgroup generated by g must include:

$0g = (0, 0)$;
$1g = (1, 1)$;
$2g = (0, 2)$;
$3g = (1, 0)$;
$4g = (0, 1)$ and
$5g = (1, 2)$.

But this includes all 6 elements of $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ and hence this group is generated by (1, 1).
It is therefore cyclic and must be isomorphic to $\mathbb{Z}_6$.

Theorem 5: If GCD(m, n) = 1 then $\mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.
Proof: Suppose GCD(m, n) = 1.
Let $g = (1, 1) \in \mathbb{Z}_m \oplus \mathbb{Z}_n$.
We shall show that g has order precisely mn.
For suppose $rg = (r, r) = (0, 0)$.
This means that r must be a multiple of m (in order to give 0 mod m).
Hence $r = mk$, for some $k \in \mathbb{Z}$.
But, by a similar argument, r must be a multiple of n.
Since m and n are coprime it follows that n divides k.
So r must be a multiple of mn. Hence the smallest value of r for which $rg = 0$ is clearly mn.

Now the group $\mathbb{Z}_m \oplus \mathbb{Z}_n$ has order mn and so it must coincide with the cyclic group generated by g, which also has order mn.
Consequently $\mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.

Example 45: $\mathbb{Z}_3 \oplus \mathbb{Z}_8 \cong \mathbb{Z}_{24}$.

Putting this another way we've shown that every finite cyclic group is isomorphic to a direct sum of cyclic groups of prime power order.

Example 46: $\mathbb{Z}_{1500} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{125}$.

Now how we decide whether two directs sums of cyclic groups are isomorphic if they have prime power orders (for the same prime)? The answer is that they are isomorphic only if the orders of the cyclic summands are the same, after possible rearrangement.

Theorem 6: Suppose $n_1, n_2, \ldots n_r, m_1, m_2, \ldots, m_s$ are all prime powers (not necessarily for the same prime) and u, v are non-negative integers. Suppose
$G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_r} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$
(u copies of $\mathbb{Z}$) where $n_1 \leq n_2 \leq \ldots$ and
$H = \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \ldots \oplus \mathbb{Z}_{m_s} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z}$
(v copies of $\mathbb{Z}$) where $m_1 \leq m_2 \leq \ldots$
Then $G \cong H$ if and only if $u = v$, $r = s$ and $n_i = m_i$ for $i = 1, 2, \ldots, r$.
Proof: The 'if' part of the proof is obvious. The 'only if' comes from considering the number of elements of each order. If the two groups are isomorphic they must have the same number of elements of each order and we can recover from these numbers, the orders of the

finite cyclic summands. We need slightly different techniques to show that $u = v$, but we omit all further details here. However in specific cases it's quite easy to do prove that the groups are not isomorphic when they differ in their direct sum decomposition. But remember, this only applies where the orders of the cyclic summands are powers of a prime.

Example 47: Show that $G = \mathbb{Z}_2 \oplus \mathbb{Z}_8$ is not isomorphic to $H = \mathbb{Z}_2 \oplus \mathbb{Z}_4$.
Solution: $|G| = 16$ while $|H| = 8$.

Example 48: Show that $G = \mathbb{Z}_2 \oplus \mathbb{Z}_8$ is not isomorphic to $H = \mathbb{Z}_4 \oplus \mathbb{Z}_4$.
Solution: G has elements of order 8 while H doesn't.

For any integer m and any prime p the group $\mathbb{Z}_{p^m}$ has exactly p elements, g, where $pg = 0$, namely $0, p^{m-1}, 2p^{m-1}, 3p^{m-1}, \ldots, (p-1)\,p^{m-1}$.

In a direct sum we multiply the numbers of such elements so that, for example, $\mathbb{Z}_{p^m} \oplus \mathbb{Z}_{p^n}$ has p^2 such elements. In general the total number of elements g with $pg = 0$, in a direct sum of cyclic groups is p^N where N is the number of finite summands whose order is divisible by p.

Example 49: Show that $G = \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8$ is not isomorphic to $H = \mathbb{Z}_8 \oplus \mathbb{Z}_8$.

Solution: G has 8 elements, g, where $2g = 0$ while H has only 4 such elements.

Example 50: Show that $G = \mathbb{Z}_4 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_8$ is not isomorphic to $H = \mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_8$.
Solution: Both groups have order 128 and both have 3 direct summands, and hence 2^3 elements of order 2. Moreover both have elements of order 8.
But G has $4 \times 4 \times 4 = 64$ elements, g, where $4g = 0$ while H has only $2 \times 4 \times 4 = 32$ such elements.

EXERCISES FOR CHAPTER 9

Exercise 1: Write down the relation matrix for the group
$[a, b, c, d \mid 6a + 7b = 2c + 11d, 12a - 6c = 27d - 18b, 3c + 9d = 3a + 6b]$

Exercise 2: Write the group $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 & 0 \\ 0 & 0 & 25 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$ as a direct sum of cyclic groups.

Exercise 3: Write the group in Exercise 1 as a direct sum of cyclic groups.

Exercise 4: Show that the group $\begin{bmatrix} 5 & 12 & 27 \\ 0 & 2 & 0 \\ 5 & 12 & 34 \end{bmatrix}$ is cyclic. Find its order.

Exercise 5: Show that the group $\begin{bmatrix} 5 & 7 & 12 \\ 7 & 16 & 21 \\ 9 & 25 & 30 \end{bmatrix}$ is cyclic. Find its order.

SOLUTIONS FOR CHAPTER 9

Exercise 1: $\begin{bmatrix} 6 & 7 & -2 & -11 \\ 12 & 18 & -6 & -27 \\ 3 & 6 & -3 & -9 \end{bmatrix}$

Exercise 2: $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 & 0 \\ 0 & 0 & 25 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \cong \mathbb{Z}_5 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z} \oplus \mathbb{Z}.$

Exercise 3:

$\begin{bmatrix} 6 & 7 & -2 & -11 \\ 12 & 18 & -6 & -27 \\ 3 & 6 & -3 & -9 \end{bmatrix} \cong \begin{bmatrix} 2 & 11 & 6 & 7 \\ 6 & 27 & 12 & 18 \\ 3 & 9 & 3 & 6 \end{bmatrix}$ by rearranging the columns and changing the sign of two of them.

This brings the component with smallest positive absolute value to the top left corner.

$\begin{bmatrix} 2 & 11 & 6 & 7 \\ 6 & 27 & 12 & 18 \\ 3 & 9 & 3 & 6 \end{bmatrix} \cong \begin{bmatrix} 2 & 11 & 6 & 7 \\ 0 & -6 & -6 & -3 \\ 1 & -2 & -3 & -1 \end{bmatrix}$ by subtracting suitable multiples of row 1 from rows 2 and 3.

$\begin{bmatrix} 2 & 11 & 6 & 7 \\ 0 & -6 & -6 & -3 \\ 1 & -2 & -3 & -1 \end{bmatrix} \cong \begin{bmatrix} 1 & -2 & -3 & -1 \\ 2 & 11 & 6 & 7 \\ 0 & -6 & -6 & -3 \end{bmatrix}$ by rearranging rows.

$$\begin{bmatrix} 1 & -2 & -3 & -1 \\ 2 & 11 & 6 & 7 \\ 0 & -6 & -6 & -3 \end{bmatrix} \cong \begin{bmatrix} 1 & -2 & -3 & -1 \\ 0 & 15 & 9 & 9 \\ 0 & 6 & 6 & 3 \end{bmatrix}$$ by subtracting twice the 1st row from the 2nd, and then changing the sign of the 3rd row.

$$\begin{bmatrix} 1 & -2 & -3 & -1 \\ 0 & 15 & 9 & 9 \\ 0 & 6 & 6 & 3 \end{bmatrix} \cong \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 15 & 9 & 9 \\ 0 & 6 & 6 & 3 \end{bmatrix}$$ by subtracting suitable multiples of the 1st column from the others.

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 15 & 9 & 9 \\ 0 & 6 & 6 & 3 \end{bmatrix} \cong \begin{bmatrix} 15 & 9 & 9 \\ 6 & 6 & 3 \end{bmatrix}$$

$$\cong \begin{bmatrix} 9 & 9 & 15 \\ 3 & 6 & 6 \end{bmatrix}$$

$$\cong \begin{bmatrix} 3 & 6 & 6 \\ 9 & 9 & 15 \end{bmatrix}$$

$$\cong \begin{bmatrix} 3 & 6 & 6 \\ 0 & -9 & -3 \end{bmatrix}$$

$$\cong \begin{bmatrix} 3 & 0 & 0 \\ 0 & -9 & -3 \end{bmatrix}$$

$$\cong \mathbb{Z}_3 \oplus [9, 3]$$

$$\cong \mathbb{Z}_3 \oplus [3, 9]$$

$$\cong \mathbb{Z}_3 \oplus [3, 0]$$

$$\cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}.$$

Exercise 4: $\begin{bmatrix} 5 & 12 & 27 \\ 0 & 2 & 0 \\ 5 & 12 & 34 \end{bmatrix} \cong \begin{bmatrix} 5 & 12 & 27 \\ 0 & 2 & 0 \\ 0 & 0 & 7 \end{bmatrix}$ by subtracting the 1st row from the 3rd

$\cong \begin{bmatrix} 5 & 2 & 7 \\ 0 & 2 & 0 \\ 0 & 0 & 7 \end{bmatrix}$ by subtracting suitable multiples of the 1st column from the others

$\cong \begin{bmatrix} 5 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 7 \end{bmatrix} \cong \mathbb{Z}_5 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_7 \cong \mathbb{Z}_{70}$ since 2, 5 and 7 are coprime.

Notice that we departed slightly from the standard algorithm. Instead of moving the '2', as the smallest positive component, to the top left hand corner, we used other operations because we could see that in this case it would simplify the arithmetic.

Exercise 5: $\begin{bmatrix} 5 & 7 & 12 \\ 7 & 16 & 21 \\ 9 & 25 & 30 \end{bmatrix} \cong \begin{bmatrix} 5 & 7 & 12 \\ 2 & 9 & 9 \\ 4 & 18 & 18 \end{bmatrix}$

$\cong \begin{bmatrix} 2 & 9 & 9 \\ 5 & 7 & 12 \\ 4 & 18 & 18 \end{bmatrix}$

$\cong \begin{bmatrix} 2 & 9 & 9 \\ 1 & -11 & -6 \\ 0 & 7 & 7 \end{bmatrix}$

$\cong \begin{bmatrix} 1 & -11 & -6 \\ 2 & 9 & 9 \\ 0 & 7 & 7 \end{bmatrix}$

$\cong \begin{bmatrix} 1 & -11 & -6 \\ 0 & 31 & 21 \\ 0 & 7 & 7 \end{bmatrix}$

$$
\begin{aligned}
&\cong \begin{bmatrix} 1 & 0 & 0 \\ 0 & 31 & 21 \\ 0 & 7 & 7 \end{bmatrix} \\
&\cong \begin{bmatrix} 31 & 21 \\ 7 & 7 \end{bmatrix} \\
&\cong \begin{bmatrix} 7 & 7 \\ 31 & 21 \end{bmatrix} \\
&\cong \begin{bmatrix} 7 & 7 \\ 3 & -7 \end{bmatrix} \\
&\cong \begin{bmatrix} 3 & -7 \\ 7 & 7 \end{bmatrix} \\
&\cong \begin{bmatrix} 3 & -7 \\ 1 & 21 \end{bmatrix} \\
&\cong \begin{bmatrix} 1 & 21 \\ 3 & -7 \end{bmatrix} \\
&\cong \begin{bmatrix} 1 & 21 \\ 0 & -70 \end{bmatrix} \\
&\cong [70] \\
&\cong \mathbb{Z}_{70}.
\end{aligned}
$$