

Basic Theory of Additive Abelian Groups

In this chapter we discuss cyclic groups, the quotient group construction, the direct sum construction and the first isomorphism theorem, in the context of additive abelian groups; we also discuss free modules. These concepts are necessary, as well as the matrix theory of Chapter 1, for the study of finitely generated abelian groups in Chapter 3. At the same time the material provides the reader with a taster for general group theory.

2.1 Cyclic \mathbb{Z} -Modules

We begin with a brief review of abelian groups. They arise in additive and multiplicative notation. Additive notation is more suited to our purpose and we'll adopt it wherever possible. The term \mathbb{Z} -module is simply another name for an additive abelian group. However it signals an approach which emphasises the analogy between vector spaces and abelian groups. The structure-preserving mappings of abelian groups, their *homomorphisms* in other words, are analogous to linear mappings of vector spaces. So in a sense the reader will have seen it all before. But be careful as the analogy is by no means perfect! For instance from $\lambda v = 0$ in a vector space one can safely deduce that either $\lambda = 0$ or $v = 0$ (or both). By contrast, in a \mathbb{Z} -module the equation $mg = 0$ may hold although $m \neq 0$ and $g \neq 0$ as we will see.

Next we study cyclic groups, that is, groups generated by a single element. Their theory is not too abstract and should help the reader's appreciation of the more general theorems on \mathbb{Z} -modules later in Chapter 2.

Let $(G, +)$ denote a set G with a binary operation denoted by addition. So G is *closed under addition*, that is,

$$g_1 + g_2 \in G \quad \text{for all } g_1, g_2 \in G.$$

Then $(G, +)$ is an (additive) abelian group if the following laws hold:

1. *The associative law of addition:* $(g_1 + g_2) + g_3 = g_1 + (g_2 + g_3)$ for all $g_1, g_2, g_3 \in G$.
2. *The existence of a zero element:* there is an element, denoted by 0, in G satisfying $0 + g = g$ for all $g \in G$.
3. *The existence of negatives:* for each $g \in G$ there is an element, denoted by $-g$, in G satisfying $-g + g = 0$.
4. *The commutative law of addition:* $g_1 + g_2 = g_2 + g_1$ for all $g_1, g_2 \in G$.

We now drop the notation $(G, +)$ and in its place refer simply to the abelian group G , the binary operation of addition being taken for granted. Laws 1, 2, 3 are *the group axioms* in additive notation. The reader should know that the zero element 0 of a group G is unique, that is, given laws 1, 2 and 3 then there is only one element 0 as in law 2. Similarly each element g of a group G has a unique negative $-g$. Laws 3 and 4 give $g + (-g) = 0$ which tells us that g is the negative of $-g$, that is, all elements g of an additive abelian group G satisfy the unsurprising equation $-(-g) = g$.

The reader might like to simplify the expression $((-g_1) + (-g_2)) + (g_1 + g_2)$ where g_1 and g_2 are elements of an additive abelian group G , using at each step one of the above four laws (start by applying law 4 followed by law 1 (twice) and then law 3, etc.). After six steps you should get the zero element 0 of G . The conclusion is: $(-g_1) + (-g_2)$ is the negative of $g_1 + g_2$ by law 3, as the sum of these two elements of G is zero. In other words $(-g_1) + (-g_2) = -(g_1 + g_2)$ for all g_1 and g_2 in G . Luckily the manipulation of elements of an additive group need not involve the laborious application of its laws as we now explain.

Let g_1, g_2, \dots, g_n be elements of an additive group G where $n \geq 3$. These elements can be summed (added up) in order in various ways, but all ways produce the same element of G . In the case $n = 4$

$$\begin{aligned} ((g_1 + g_2) + g_3) + g_4 &= ((g_1 + (g_2 + g_3)) + g_4 = g_1 + ((g_2 + g_3) + g_4) \\ &= g_1 + (g_2 + (g_3 + g_4)) = (g_1 + g_2) + (g_3 + g_4) \end{aligned}$$

using only law 1. Omitting the brackets we see that $g_1 + g_2 + g_3 + g_4$ has an unambiguous meaning, namely any one of the above (equal) elements. Using law 1 and induction on n , it can be shown (Exercises 2.1, Question 8(a)) that brackets may be left out when adding up, in order, any finite number n of elements g_1, g_2, \dots, g_n of an additive group G to give *the generalised associative law of addition*. So the sum $g_1 + g_2 + \dots + g_n$ of n elements of an additive abelian group G is unambiguously defined and what is more this sum is unchanged when the suffixes are permuted (*the generalised commutative law of addition*). In the case $n = 3$

$$\begin{aligned} g_1 + g_2 + g_3 &= g_1 + g_3 + g_2 = g_3 + g_1 + g_2 \\ &= g_3 + g_2 + g_1 = g_2 + g_3 + g_1 = g_2 + g_1 + g_3. \end{aligned}$$

Let g be an element of an additive abelian group G . The elements $2g = g + g$, $3g = g + g + g$ belong to G . More generally for every positive integer n the group element ng is obtained by adding together n elements equal g , that is,

$$ng = g + g + \cdots + g \quad (n \text{ terms}).$$

So $1g = g$ and as $n(-g) + ng = 0$ we deduce that $n(-g) = -(ng)$. Therefore it makes sense to define $(-n)g$ to be the group element $n(-g)$ and to define $0g$ to be the zero element 0 of G . It follows that $(-n)(-g) = n(-(-g)) = ng$. But more importantly we have given meaning to mg for *all* integers m (positive, negative and zero) and all elements g in G and

$$mg \in G \quad \text{for all } m \in \mathbb{Z}, g \in G$$

showing that G is *closed* under *integer multiplication*.

Integer multiplication on G and the group operation of addition on G are connected by the following laws:

5. *The distributive laws:*

$$\begin{aligned} m(g_1 + g_2) &= mg_1 + mg_2 \quad \text{for all } m \in \mathbb{Z} \text{ and all } g_1, g_2 \in G, \\ (m_1 + m_2)g &= m_1g + m_2g \quad \text{for all } m_1, m_2 \in \mathbb{Z} \text{ and all } g \in G. \end{aligned}$$

6. *The associative law of multiplication:*

$$(m_1m_2)g = m_1(m_2g) \quad \text{for all } m_1, m_2 \in \mathbb{Z} \text{ and all } g \in G.$$

7. *The identity law:* $1g = g$ for all $g \in G$.

Laws 5 and 6 are the familiar laws of indices expressed in additive notation, rather than the more usual multiplicative notation; they allow elements of additive abelian groups to be manipulated with minimum fuss (see Exercises 2.1, Question 8(c)). Law 7 is frankly something of an anti-climax, but its presence will help us generalise these ideas later in a coherent way. The structure of G is expressed concisely by saying

$$G \text{ is a } \mathbb{Z}\text{-module}$$

meaning that laws 1–7 above hold. Notice the close connection between the laws of a \mathbb{Z} -module and the laws of a vector space: they are almost identical! Think of the elements of G as being ‘vectors’ and the elements of \mathbb{Z} as being ‘scalars’. The only thing which prevents a \mathbb{Z} -module from being a vector space is the fact that \mathbb{Z} is not a field.

The reader will already have met many examples of additive abelian groups: for example the additive group $(\mathbb{Q}, +)$ of all rational numbers m/n ($m, n \in \mathbb{Z}, n > 0$);

this group is obtained from the rational field \mathbb{Q} by ignoring products of non-integer rational numbers – they simply don't arise in $(\mathbb{Q}, +)$. In the same way, ignoring the multiplication on any ring R , we obtain its *additive group* $(R, +)$. Of particular importance are the additive groups of the *residue class rings* \mathbb{Z}_n (we'll shortly review their properties) as well as the additive group of the ring \mathbb{Z} itself.

Let H be a *subgroup* of the additive abelian group G . So H is a subset of G satisfying

- (a) $h_1 + h_2 \in H$ for all $h_1, h_2 \in H$ (H is closed under addition)
- (b) $0 \in H$ (H contains the zero element of G)
- (c) $-h \in H$ for all $h \in H$ (H is closed under negation).

By (a) we see that H is a set with a binary operation of addition and so it makes sense to ask: is $(H, +)$ an abelian group? As $H \subseteq G$ and law 1 holds in G , we see that $(h_1 + h_2) + h_3 = h_1 + (h_2 + h_3)$ for all h_1, h_2, h_3 in H , that is, law 1 holds in H . In the same way law 4 holds in H . Also (b) and (c) ensure that law 2 and law 3 hold in H . So $(H, +)$ is an abelian group as laws 1–4 hold with G replaced by H . Hence laws 5, 6 and 7 also hold with G replaced by H , that is, H is a \mathbb{Z} -module. The relationship between H and G is described by saying

H is a submodule of the \mathbb{Z} -module G .

The set $\langle 2 \rangle$ of even integers is a subgroup of the additive group \mathbb{Z} and so $\langle 2 \rangle$ is a submodule of \mathbb{Z} . The discussion preceding Theorem 1.15 shows that $\langle 2 \rangle$ is an ideal of the ring \mathbb{Z} . More generally H is a *submodule* of the \mathbb{Z} -module \mathbb{Z} if and only if H is an *ideal* of the ring \mathbb{Z} , and when this is the case Theorem 1.15 tells us $H = \langle d \rangle$ where d is a non-negative integer.

We now discuss in detail *cyclic* \mathbb{Z} -modules. They are crucial: on the one hand they and their submodules are easily described as we will soon see, and on the other hand every finitely generated \mathbb{Z} -module can be constructed using them as building blocks, as we show in Section 3.1.

Definition 2.1

Let G be a \mathbb{Z} -module containing an element g such that every element of G is of the type mg for some $m \in \mathbb{Z}$. Then G is said to be *cyclic* with *generator* g and we write $G = \langle g \rangle$.

The additive group \mathbb{Z} of all integers is a cyclic \mathbb{Z} -module with generator 1 and so $\mathbb{Z} = \langle 1 \rangle$. As \mathbb{Z} contains an infinite number of elements we say that \mathbb{Z} is an *infinite cyclic group*. Let K be a subgroup of \mathbb{Z} (we know that subgroups of \mathbb{Z} are ideals Theorem 1.15 and so we denote them by K rather than H). As $K = \langle d \rangle$ where d is non-negative, every subgroup K of the infinite cyclic group \mathbb{Z} is itself cyclic because

K has generator d . Note that $-d$ is also a generator of K as $\langle -d \rangle = \langle d \rangle$. The subgroup $\langle 2 \rangle$ of all even integers is infinite cyclic just like its ‘parent’ \mathbb{Z} and the same is true of $\langle d \rangle$ with $d \neq 0$. Notice that $\langle 6 \rangle \subseteq \langle 2 \rangle$ as 2 is a divisor of 6 and so all integer multiples of 6 are even integers. More generally $\langle d_1 \rangle \subseteq \langle d_2 \rangle$ if and only if $d_2 | d_1$, where $d_1, d_2 \in \mathbb{Z}$.

Let n be a positive integer. The reader is assumed to have met the ring \mathbb{Z}_n of integers modulo n ; however, we now briefly review its construction and properties. A typical element of \mathbb{Z}_n is the congruence class \bar{r} of an integer r , that is, $\bar{r} = \{nq + r : q \in \mathbb{Z}\}$. So \bar{r} is the subset of integers $m = nq + r$ which differ from r by an integer multiple q of n . Therefore $m - r = nq$, that is, the difference between m and r is divisible by n ; this is expressed by saying that m is congruent to r modulo n and writing $m \equiv r \pmod{n}$. So \mathbb{Z}_n has n elements and

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

since the n congruence classes \bar{r} correspond to the n possible remainders r on dividing an arbitrary integer m by n . You should know that \mathbb{Z}_n is a commutative ring, the rules of addition and multiplication being unambiguously defined by $\overline{m} + \overline{m'} = \overline{m + m'}$, $(\overline{m})(\overline{m'}) = \overline{mm'}$ for all $m, m' \in \mathbb{Z}$. The 0-element and 1-element of \mathbb{Z}_n are $\bar{0}$ and $\bar{1}$ respectively. You should also know that \mathbb{Z}_n is a field if and only if n is prime. The smallest field is $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ having two elements, namely the set $\bar{0}$ of all even integers and the set $\bar{1}$ of all odd integers.

The additive group of \mathbb{Z}_n is cyclic, being generated by $\bar{1}$ as $\overline{m} = m\bar{1}$. Having n elements, \mathbb{Z}_n is a cyclic group of order n .

For example, taking $n = 4$ we obtain the cyclic group $\mathbb{Z}_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ of order 4 with addition table:

| + | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|-----------|-----------|-----------|-----------|-----------|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |

The element $x + y$ appears in the table where the row headed by x meets the column headed by y , for $x, y \in \mathbb{Z}_4$. By inspection \mathbb{Z}_4 has three subgroups $\{\bar{0}\}$, $\{\bar{0}, \bar{2}\}$ and \mathbb{Z}_4 itself. The union of the congruence classes belonging to any one of these subgroups of \mathbb{Z}_4 is a subgroup of \mathbb{Z} . Thus $\bar{0} = \langle 4 \rangle$ since $\bar{0}$ consists of integers which are multiples of 4. Similarly $\bar{0} \cup \bar{2} = \langle 2 \rangle$ since $\bar{2}$ consists of integers which are multiples of 2 but not multiples of 4. Also $\bar{0} \cup \bar{1} \cup \bar{2} \cup \bar{3} = \mathbb{Z} = \langle 1 \rangle$. The three subgroups of \mathbb{Z}_4 correspond in this way to the three subgroups $\langle 4 \rangle$, $\langle 2 \rangle$, $\langle 1 \rangle$ of \mathbb{Z} which contain $\langle 4 \rangle$. What is more, the subgroups of \mathbb{Z}_4 are cyclic with generators $\bar{4}$, $\bar{2}$, $\bar{1}$. We now return to \mathbb{Z}_n and show that these ideas can be generalised.

Lemma 2.2

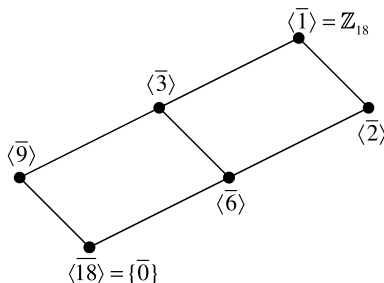
Let n be a positive integer. Each subgroup H of the additive group \mathbb{Z}_n is cyclic with generator \bar{d} where $d|H| = n$ and $|H|$ is the number of elements in H .

Proof

For each subgroup H of \mathbb{Z}_n let $K = \{m \in \mathbb{Z} : \bar{m} \in H\}$. So K consists of those integers m which belong to a congruence class in H . We show that K is a subgroup of \mathbb{Z} containing $\langle n \rangle$. Let $m_1, m_2 \in K$. Then $\bar{m}_1, \bar{m}_2 \in H$. As H is closed under addition, $\overline{m_1 + m_2} = \bar{m}_1 + \bar{m}_2 \in H$. So $m_1 + m_2 \in K$ showing that K is closed under addition. Now $\bar{0} \in H$ as H contains the zero element of \mathbb{Z}_n . But $\bar{0}$ consists of all integer multiples of n . So $\bar{0} = \langle n \rangle \subseteq K$ and in particular $0 \in K$. Let $m \in K$. Then $\bar{m} \in H$ and so $\overline{-m} = -\bar{m} \in H$ as H is closed under negation. Therefore $-m \in K$ showing that K is closed under negation. We have shown that K is a subgroup of \mathbb{Z} containing $\langle n \rangle$. So $K = \langle d \rangle$ for some non-negative integer d by Theorem 1.15. As $\langle n \rangle \subseteq \langle d \rangle$ we conclude that $d|n$. As n is positive, d cannot be zero and so d is positive also. As $d \in K$ we see that $\bar{d} \in H$. Finally consider $\bar{m} \in H$. Then $m \in K$ and so $m = qd$ for some $q \in \mathbb{Z}$. So $\bar{m} = q\bar{d}$ showing that H is cyclic with generator \bar{d} .

Now $|H|$ is the order of H (the number of elements in H) and so K is the union of $|H|$ congruence classes (mod n). Let $m \in K$. As $K = \langle d \rangle$ there is $q \in \mathbb{Z}$ with $m = qd$. Divide q by n/d to obtain integers q', r with $q = q'(n/d) + r$ where $0 \leq r < n/d$. Then $m = (q'(n/d) + r)d = q'n + rd$, showing that K consists of the n/d congruence classes \bar{rd} . Hence $|H| = n/d$ and so $d|H| = n$. \square

For example, by Lemma 2.2 the additive group \mathbb{Z}_{18} has 6 subgroups corresponding to the 6 positive divisors 1, 2, 3, 6, 9, 18, of 18.



These 6 subgroups can be arranged in their lattice diagram, as shown, in which subgroup H_1 is contained in subgroup H_2 if and only if there is a sequence of upwardly sloping lines joining H_1 to H_2 . For instance $\bar{6} \subseteq \bar{1}$ but $\bar{9} \not\subseteq \bar{2}$.

The proof of Lemma 2.2 shows that each subgroup H of \mathbb{Z}_n corresponds to a subgroup K of \mathbb{Z} which contains $\langle n \rangle$. From the last paragraph we see that each such subgroup K has a positive generator d and is made up of n/d congruence classes $(\text{mod } n)$. These n/d elements form a subgroup H of \mathbb{Z}_n . So for each K there is one H and vice-versa. We show in Theorem 2.17 that bijective correspondences of this type arise in a general context. To get the idea, consider

the natural mapping $\eta : \mathbb{Z} \rightarrow \mathbb{Z}_n$

which maps each integer m to its congruence class \overline{m} modulo n . We use $(m)\eta$ to denote the image of m by η and so $(m)\eta = \overline{m}$ for all integers m . Now η is *additive*, that is,

$$(m + m')\eta = (m)\eta + (m')\eta \quad \text{for all } m, m' \in \mathbb{Z}$$

as $\overline{m + m'} = \overline{m} + \overline{m'}$. Such additive mappings provide meaningful comparisons between additive abelian groups and surprisingly each one gives rise to a bijective correspondence as above. The *image* of η is the set of all elements $(m)\eta$ and is denoted by $\text{im } \eta$. As η is surjective (onto) we see $\text{im } \eta = \mathbb{Z}_n$. The *kernel* of η is the set of elements m such that $(m)\eta = \overline{0}$, the zero element of \mathbb{Z}_n , and is denoted by $\ker \eta$. So $\ker \eta = \langle n \rangle$. With this terminology the correspondence between H and K , where $K = \{m \in \mathbb{Z} : (m)\eta \in H\}$, is bijective from the set of subgroups H of $\text{im } \eta$ to the set of subgroups K of \mathbb{Z} which contain $\ker \eta$. We take up this theme in Theorem 2.17.

Definition 2.3

Let G and G' be additive abelian groups. A mapping $\theta : G \rightarrow G'$ such that $(g_1 + g_2)\theta = (g_1)\theta + (g_2)\theta$ for all $g_1, g_2 \in G$ is called *additive* or a *homomorphism*.

Such mappings θ respect the group operation and satisfy $(0)\theta = 0'$, $(-g)\theta = -(g)\theta$ for $g \in G$, that is, θ maps the zero of G to the zero of G' and θ respects negation (see Exercises 2.1, Question 4(c)). With $g_1 = g_2 = g$ in Definition 2.3 we obtain $(2g)\theta = 2((g)\theta)$. Using induction the additive mapping θ satisfies

$$(mg)\theta = m((g)\theta)$$

for all $m \in \mathbb{Z}$, $g \in G$. We describe θ as being *\mathbb{Z} -linear*, meaning that θ is additive and satisfies the above equation, that is, θ maps each integer multiple mg of each element g of G to m times the element $(g)\theta$ of G' .

The natural mapping $\eta : \mathbb{Z} \rightarrow \mathbb{Z}_n$ is \mathbb{Z} -linear. The ‘doubling’ mapping $\theta : \mathbb{Z} \rightarrow \mathbb{Z}$, where $(m)\theta = 2m$ for all $m \in \mathbb{Z}$, is also \mathbb{Z} -linear.

How can we tell whether two \mathbb{Z} -modules are really different or essentially the same? The next definition provides the terminology to tackle this problem.

Definition 2.4

A bijective (one-to-one and onto) \mathbb{Z} -linear mapping is called an *isomorphism*. The \mathbb{Z} -modules G and G' are called *isomorphic* if there is an isomorphism $\theta : G \rightarrow G'$ in which case we write $\theta : G \cong G'$ or simply $G \cong G'$. An isomorphism $\theta : G \cong G$ of G to itself is called an *automorphism* of G .

For example $\theta : \mathbb{Z} \cong \langle 2 \rangle$, where $(m)\theta = 2m$ for all $m \in \mathbb{Z}$, is an isomorphism showing that the \mathbb{Z} -module of all integers is isomorphic to the \mathbb{Z} -module of all even integers. In the same way $\mathbb{Z} \cong \langle d \rangle$ for every non-zero integer d . Isomorphic \mathbb{Z} -modules are abstractly identical and differ at most in notation.

The inverse of an isomorphism $\theta : G \cong G'$ is an isomorphism $\theta^{-1} : G' \cong G$ and the composition of compatible isomorphisms $\theta : G \cong G'$ and $\theta' : G' \cong G''$ is an isomorphism $\theta\theta' : G \cong G''$ (Exercises 2.1, Question 4(d)).

The additive cyclic group \mathbb{Z} is generated by 1 and also by -1 . As \mathbb{Z} has no other generators there is just one non-identity automorphism of \mathbb{Z} , namely $\tau : \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $(m)\tau = -m$ for all $m \in \mathbb{Z}$. Notice that $(1)\tau = -1$ and $(-1)\tau = 1$. More generally, every automorphism of a cyclic group permutes the generators amongst themselves.

Let g be an element of the additive group G . The *smallest* positive integer n such that $ng = 0$ is called the *order* of g ; if there is no such integer n then g is said to have *infinite* order. We now reformulate this concept in a more convenient manner – it will enable finite and infinite cyclic groups to be dealt with in a unified way.

Let $K = \{m \in \mathbb{Z} : mg = 0\}$, that is, K consists of those integers m such that mg is the zero element of G . It's routine to show that K is an ideal of \mathbb{Z} . So K is a principal ideal of \mathbb{Z} with non-negative generator n , that is, $K = \langle n \rangle$ by Theorem 1.15. Then $n = 0$ means that g has infinite order whereas $n > 0$ means that g has finite order n . The ideal $K = \langle n \rangle$ is called the *order ideal* of g . Notice

$$mg = 0 \quad \Leftrightarrow \quad m \in K \quad \Leftrightarrow \quad n|m$$

which is a useful criterion for finding the order of a group element in particular cases. For instance suppose $36g = 0$, $18g \neq 0$, $12g \neq 0$. Then g has order n such that n is a divisor of 36 but not a divisor of either $18 = 36/2$ or $12 = 36/3$. There is only one such positive integer n , namely 36. So g has order 36. More generally

$$g \text{ has finite order } n \quad \Leftrightarrow \quad ng = 0 \quad \text{and} \quad (n/p)g \neq 0 \quad \text{for all prime divisors } p \text{ of } n.$$

The \Leftarrow implication is valid because every positive divisor d of n with $d < n$ satisfies $d|(n/p)$ for some prime divisor p of n ; so d cannot be the order of g , and hence n is the order of g .

Be careful! From $24g = 0$ and $12g \neq 0$ one cannot deduce that g has order 24, as g could have order 8.

Once again let g be an element of the additive group G . Then $\langle g \rangle = \{mg : m \in \mathbb{Z}\}$ is a subgroup of G . As $\langle g \rangle$ is cyclic with generator g it is reasonable to call $\langle g \rangle$ *the cyclic subgroup of G generated by g* .

We now explain how the order ideal K of a group element g determines the *isomorphism type* Definition 2.6 of the cyclic group $\langle g \rangle$.

Theorem 2.5

Every cyclic group G is isomorphic either to the additive group \mathbb{Z} or to the additive group \mathbb{Z}_n for some positive integer n .

Proof

Let g generate G and so $G = \langle g \rangle$. Consider $\theta : \mathbb{Z} \rightarrow G$ defined by $(m)\theta = mg$ for all integers m . Then θ is \mathbb{Z} -linear by laws 5 and 6 of a \mathbb{Z} -module. Now θ is surjective (onto) since every element of G is of the form $(m)\theta$ for some $m \in \mathbb{Z}$, that is, $\text{im } \theta = G$ meaning that G is the image of θ (we'll state the general definition of image and kernel in Section 2.3). The kernel of θ is $\ker \theta = \{m \in \mathbb{Z} : (m)\theta = 0\} = \{m \in \mathbb{Z} : mg = 0\} = K$ which is the order ideal of g . By Theorem 1.15 there is a non-negative integer n with $\ker \theta = \langle n \rangle$.

Suppose $n = 0$. Then θ is injective (one-to-one) because suppose $(m)\theta = (m')\theta$. Then $(m - m')\theta = (m)\theta - (m')\theta = 0$ showing that $m - m'$ belongs to $\ker \theta = \langle 0 \rangle = \{0\}$. So $m - m' = 0$, that is, $m = m'$. Therefore θ is bijective and so $\theta : \mathbb{Z} \cong G$, that is,

all infinite cyclic groups are isomorphic to the additive group \mathbb{Z} of integers.

Suppose $n > 0$. As above we suppose $(m)\theta = (m')\theta$. This means $m - m' \in \ker \theta = K = \langle n \rangle$ and so $m - m'$ is an integer multiple of n , that is, $m \equiv m' \pmod{n}$. The steps can be reversed to show that $m \equiv m' \pmod{n}$ implies $(m)\theta = (m')\theta$. So θ has the same effect on integers m and m' which are congruent \pmod{n} . In other words θ has the same effect on all the integers of each congruence class \overline{m} , and it makes sense to introduce the mapping $\tilde{\theta} : \mathbb{Z}_n \rightarrow G$ defined by $(\overline{m})\tilde{\theta} = (m)\theta$ for all $m \in \mathbb{Z}$. As θ is additive and surjective, the same is true of $\tilde{\theta}$. As θ has different effects on different congruence classes \pmod{n} , we see that $\tilde{\theta}$ is injective. Therefore $\tilde{\theta} : \mathbb{Z}_n \cong G$ which shows:

every cyclic group of finite order n is isomorphic to the additive group \mathbb{Z}_n . \square

We will see in Theorem 2.16 that every \mathbb{Z} -linear mapping θ gives rise to an isomorphism $\tilde{\theta}$ as in the above proof. To illustrate Theorem 2.5 let $g = \overline{18} \in \mathbb{Z}_{60}$. The

order of g is the smallest positive integer n satisfying $18n \equiv 0 \pmod{60}$. Dividing through by $\gcd\{18, 60\} = 6$ we obtain $3n \equiv 0 \pmod{10}$ and so $n = 10$. Therefore g has order 10 and hence generates a subgroup $\langle g \rangle$ of \mathbb{Z}_{60} which is isomorphic to the additive group \mathbb{Z}_{10} by Theorem 2.5. The reader can check

$$\langle g \rangle = \{\overline{0}, \overline{18}, \overline{36}, \overline{54}, \overline{12}, \overline{30}, \overline{48}, \overline{6}, \overline{24}, \overline{42}\} \subseteq \mathbb{Z}_{60}$$

and $\tilde{\theta} : \mathbb{Z}_{10} \cong \langle g \rangle$ where $(\overline{m})\tilde{\theta} = \overline{18m}$ for $\overline{m} \in \mathbb{Z}_{10}$.

From the proof of Theorem 2.5 we see

$$g \text{ has finite order } n \quad \Leftrightarrow \quad |\langle g \rangle| = n$$

In other words, each element g of finite order n generates a cyclic subgroup $\langle g \rangle$ of order n .

Definition 2.6

Let n be a positive integer. A cyclic \mathbb{Z} -module G is said to be of *isomorphism type* C_n or C_0 according as G is isomorphic to the additive group \mathbb{Z}_n or the additive group \mathbb{Z} .

So for $n > 0$, groups of isomorphism type C_n are cyclic groups of order n . Groups of type C_0 are infinite cyclic groups. Groups of type C_1 are *trivial* because they contain only one element, namely their zero element. Notice that for all non-negative integers n

$$G = \langle g \rangle \text{ has isomorphism type } C_n \text{ where } \langle n \rangle \text{ is the order ideal of } g$$

How is the order of mg related to the order of g ? Should g have infinite order then mg also has infinite order for $m \neq 0$ and order 1 for $m = 0$.

Lemma 2.7

Let the \mathbb{Z} -module element g have finite order n . Then mg has finite order $n/\gcd\{m, n\}$ for $m \in \mathbb{Z}$.

Proof

The order ideal of g is $\langle n \rangle$. Let $\langle n' \rangle$ be the order ideal of mg where $n' \geq 0$. Write $d = \gcd\{m, n\}$. Then $(n/d)mg = (m/d)ng = (m/d)0 = 0$ showing that n/d annihilates mg , that is, n/d belongs to the order ideal $\langle n' \rangle$ of mg . Hence n' is a divisor of n/d and also $n' > 0$. On the other hand $n'mg = 0$ shows that $n'm$ belongs to the order ideal $\langle n \rangle$ of g . So $n'm = qn$ for some integer q . Hence n/d is a divisor of n' (m/d). But m/d

and n/d are *coprime integers* meaning $\gcd\{m/d, n/d\} = 1$. Hence n/d is a divisor of n' . As n/d and n' are both positive and each is a divisor of the other we conclude that $n' = n/d$. So mg has order $n' = n/d = n/\gcd\{m, n\}$. \square

For example the element $\bar{1}$ of the additive group \mathbb{Z}_{60} has order 60. So $\overline{18} = 18(\bar{1})$ in \mathbb{Z}_{60} has order $60/\gcd\{18, 60\} = 60/6 = 10$. As we saw earlier, $\overline{18}$ generates a cyclic subgroup of \mathbb{Z}_{60} with $|\langle \overline{18} \rangle| = 10$. We will see in Section 3.1 that Lemma 2.7 plays an crucial part in the theory of finite abelian groups.

Finally we work through an application of these ideas which involves an abelian group in *multiplicative* notation. This abelian group is familiar to the reader yet has a hint of mystery!

Example 2.8

Let G denote the multiplicative group \mathbb{Z}_{43}^* of non-zero elements of the field \mathbb{Z}_{43} . In Corollary 3.17 it is shown that the multiplicative group F^* of every finite field F is cyclic. So \mathbb{Z}_p^* is cyclic for all primes p . In particular \mathbb{Z}_{43}^* is cyclic, and we set out to find a generator by ‘trial and error’. As $|G| = 42 = 2 \times 3 \times 7$ each generator g has order 42, that is, $g^{42} = \bar{1}$ the identity element of \mathbb{Z}_{43}^* , and $g^{42/7} = g^6 \neq \bar{1}$, $g^{42/3} = g^{14} \neq \bar{1}$, $g^{42/2} = g^{21} \neq \bar{1}$.

We first try $g = \bar{2}$. Then $g^6 = \overline{64} = \overline{21} \neq \bar{1}$, and so $g^7 = gg^6 = \bar{2} \times \overline{21} = \overline{42} = -\bar{1}$. Squaring the last equation gives $g^{14} = g^7 g^7 = (-\bar{1})^2 = \bar{1}$ showing that $\bar{2}$ is not a generator of \mathbb{Z}_{43}^* . In fact $\bar{2}$ has order 14.

Now try $g = \bar{3}$. Then $g^4 = \overline{81} = -\bar{5}$ and so $g^6 = g^4 g^2 = (-\bar{5}) \times \bar{9} = -\overline{45} = -\bar{2} \neq \bar{1}$. Hence $g^7 = g^6 g = (-\bar{2}) \times \bar{3} = -\bar{6}$. Squaring gives $g^{14} = g^7 g^7 = (-\bar{6})^2 = \overline{36} = -\bar{7} \neq \bar{1}$. Then $g^{21} = g^7 g^{14} = (-\bar{6}) \times (-\bar{7}) = \overline{42} = -\bar{1} \neq \bar{1}$. Squaring now gives $g^{42} = g^{21} g^{21} = (-\bar{1})^2 = \bar{1}$. So $g^{42} = \bar{1}$ and $g^6 \neq \bar{1}$, $g^{14} \neq \bar{1}$, $g^{21} \neq \bar{1}$ which show that g has order 42. Therefore the integer powers of $g = \bar{3}$ are the elements of a cyclic subgroup H of order 42. As $H \subseteq \mathbb{Z}_{43}^*$ and both H and \mathbb{Z}_{43}^* have exactly 42 elements, we conclude $H = \mathbb{Z}_{43}^*$. So \mathbb{Z}_{43}^* is cyclic with generator $\bar{3}$.

Having found one generator of \mathbb{Z}_{43}^* we use Lemma 2.7 to find all g with $\langle g \rangle = \mathbb{Z}_{43}^*$. There is an integer m with $g = (\bar{3})^m$ and $1 \leq m \leq 42$. Comparing orders gives $\langle g \rangle = \mathbb{Z}_{43}^* \Leftrightarrow 42 = 42/\gcd\{m, 42\} \Leftrightarrow \gcd\{m, 42\} = 1$ by Lemma 2.7. So \mathbb{Z}_{43}^* has 12 generators $g = (\bar{3})^m$ where $m \in \{1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41\}$. For instance $(\bar{3})^5 = \overline{81} \times \bar{3} = -\bar{5} \times \bar{3} = -\bar{15} = \overline{28}$ generates \mathbb{Z}_{43}^* . In Section 2.2 we will meet the *Euler ϕ -function* and see that $12 = \phi(42)$.

By *Fermat’s little theorem*, which is proved at the beginning of Section 2.2, every element $g = \bar{r}$ of $G = \mathbb{Z}_p^*$, p prime, satisfies $g^{p-1} = \bar{1}$. So

$$g \text{ is a generator of } \mathbb{Z}_p^* \Leftrightarrow g^{(p-1)/p'} \neq \bar{1} \quad \text{for all prime divisors } p' \text{ of } p-1.$$

EXERCISES 2.1

1. (a) Write out the addition table of the additive group \mathbb{Z}_5 . Does $\bar{4} \in \mathbb{Z}_5$ generate \mathbb{Z}_5 ? Which elements of \mathbb{Z}_5 are generators? Specify the (two) subgroups of \mathbb{Z}_5 .
- (b) Write out the addition table of the \mathbb{Z} -module \mathbb{Z}_6 . Express the elements $27(\bar{2})$, $-17(\bar{4})$, $15(\bar{3}) + 13(\bar{4})$ in the form \bar{r} , $0 \leq r < 6$. List the elements in each of the four submodules H of \mathbb{Z}_6 and express the corresponding submodules K of \mathbb{Z} in the form $\langle d \rangle$, $d \geq 0$. Specify a generator of each H . Which elements generate \mathbb{Z}_6 ?
Hint: Use Lemma 2.2.
- (c) List the elements in the submodule of the \mathbb{Z} -module \mathbb{Z}_{21} generated by

$$(i) \quad \bar{14}; \quad (ii) \quad \bar{15}.$$

What are the orders of $\bar{14}$ and $\bar{15}$ in \mathbb{Z}_{21} ? What common property do the 12 elements of \mathbb{Z}_{21} not in either of these submodules have?

Hint: Use Definition 2.1.

2. (a) Calculate $\gcd\{91, 289\}$. Does $\overline{91}$ generate the \mathbb{Z} -module \mathbb{Z}_{289} ? Does $\overline{51}$ generate this \mathbb{Z} -module?
Hint: Use Lemma 2.7.
- (b) Use Lemma 2.7 to show that $\overline{m} \in \mathbb{Z}_n$ is a generator of the \mathbb{Z} -module \mathbb{Z}_n if and only if $\gcd\{m, n\} = 1$.
- (c) List the elements of \mathbb{Z}_{25} which are *not* generators of the \mathbb{Z} -module \mathbb{Z}_{25} . Do these elements form a submodule of \mathbb{Z}_{25} ? How many generators does the \mathbb{Z} -module \mathbb{Z}_{125} have?
- (d) Let p be prime. Find the number of generators in each of the following \mathbb{Z} -modules:

$$(i) \quad \mathbb{Z}_p; \quad (ii) \quad \mathbb{Z}_{p^2}; \quad (iii) \quad \mathbb{Z}_{p^3}; \quad (iv) \quad \mathbb{Z}_{p^l}.$$

3. (a) Show that $\bar{2} \in \mathbb{Z}_{13}$ satisfies $(\bar{2})^4 = \bar{3}$, $(\bar{2})^6 = \overline{-1}$. Deduce that $\bar{2}$ has order 12. Express each power $(\bar{2})^l$ for $1 \leq l \leq 12$ in the form \bar{r} where $1 \leq r \leq 12$. Does $\bar{2}$ generate the multiplicative group \mathbb{Z}_{13}^* of non-zero elements of \mathbb{Z}_{13} ? Use Lemma 2.7 to find the elements \bar{r} which generate \mathbb{Z}_{13}^* .
- (b) Find a generator g of the multiplicative group \mathbb{Z}_{17}^* by 'trial and error'. Specify the 5 subgroups of \mathbb{Z}_{17}^* (each is cyclic with generator a power of g). How many generators does \mathbb{Z}_{17}^* have?
- (c) Verify that $2^8 \equiv -3 \pmod{37}$. Hence show that $\bar{2}$ generates \mathbb{Z}_{37}^* (it's not enough to show $(\bar{2})^{36} = \bar{1}$). Arrange the 9 subgroups of \mathbb{Z}_{37}^* in their lattice diagram. How many generators does \mathbb{Z}_{37}^* have?

- (d) Find the orders of each of the elements $\overline{2}, \overline{3}, \overline{4}, \overline{5}$ of \mathbb{Z}_{41}^* . Find a generator of \mathbb{Z}_{41}^* .
4. (a) Let G be a \mathbb{Z} -module and c an integer. Show that $\theta : G \rightarrow G$, given by $(g)\theta = cg$ for all $g \in G$, is \mathbb{Z} -linear.
 Let $\theta : G \rightarrow G$ be \mathbb{Z} -linear and G cyclic with generator g_0 . Show that there is an integer c as above. Let $\langle n \rangle$ be the order ideal of g_0 . Show that c is unique modulo n . Show further that θ is an automorphism of G if and only if $\gcd\{c, n\} = 1$.
 Deduce that the additive group \mathbb{Z} has exactly 2 automorphisms.
 Show that every \mathbb{Z} -linear mapping $\theta : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ for $n > 0$ is of the form $(\overline{m})\theta = \overline{c} \overline{m}$ for all $\overline{m} \in \mathbb{Z}_n$ and some $\overline{c} \in \mathbb{Z}_n$. Show also that $\theta : \mathbb{Z}_n \cong \mathbb{Z}_n$ if and only if $\gcd\{c, n\} = 1$. How many automorphisms does the additive group \mathbb{Z}_9 have? Are all of these automorphisms powers of $\theta_2 : \mathbb{Z}_9 \rightarrow \mathbb{Z}_9$ defined by $(\overline{m})\theta_2 = 2\overline{m}$ for all $\overline{m} \in \mathbb{Z}_9$?
- (b) Let G and G' be \mathbb{Z} -modules and let $\varphi : G \rightarrow G'$ be a \mathbb{Z} -linear mapping. For g_0 in G let $\langle n \rangle$ and $\langle n' \rangle$ be the order ideals of g_0 and $(g_0)\varphi$ respectively. Show that $n' | n$.
 Suppose now that $G = \langle g_0 \rangle$ and let g'_0 in G' have order ideal $\langle d \rangle$ where $d | n$. Show that there is a unique \mathbb{Z} -linear mapping $\theta : G \rightarrow G'$ with $(g_0)\theta = g'_0$.
 How many \mathbb{Z} -linear mappings $\theta : \mathbb{Z} \rightarrow \mathbb{Z}_{12}$ are there? How many of these mappings are surjective?
 Show that $\overline{r} \in \mathbb{Z}_n$ has order ideal $\langle n / \gcd\{r, n\} \rangle$ for $n > 0$. Show that the number of \mathbb{Z} -linear mappings $\theta : \mathbb{Z}_m \rightarrow \mathbb{Z}_n$ is $\gcd\{m, n\}$. Specify explicitly the five \mathbb{Z} -linear mappings $\mathbb{Z}_{10} \rightarrow \mathbb{Z}_{15}$ and the five \mathbb{Z} -linear mappings $\mathbb{Z}_{15} \rightarrow \mathbb{Z}_{10}$.
- (c) Let $\theta : G \rightarrow G'$ be a homomorphism Definition 2.3 where G and G' are abelian groups with zero elements 0 and $0'$ respectively. Show that $(0)\theta = 0'$ and $(-g)\theta = -(g)\theta$ for all $g \in G$.
- (d) Let G, G', G'' be \mathbb{Z} -modules and let $\theta : G \rightarrow G', \theta' : G' \rightarrow G''$ be \mathbb{Z} -linear mappings. Show that $\theta\theta' : G \rightarrow G''$ is \mathbb{Z} -linear where $(m)\theta\theta' = ((m)\theta)\theta' \forall m \in \mathbb{Z}$. For bijective θ show that $\theta^{-1} : G' \rightarrow G$ is \mathbb{Z} -linear. Deduce that the automorphisms of G are the elements of a multiplicative group $\text{Aut } G$, the group operation being composition of mappings. Is $\text{Aut } \mathbb{Z}_9$ cyclic? Is $\text{Aut } \mathbb{Z}_8$ cyclic?
5. (a) Let G be a \mathbb{Z} -module. Show that $H = \{2g : g \in G\}$ and $K = \{g \in G : 2g = 0\}$ are submodules of G . Find examples of G with
- (i) $H \subset K$; (ii) $H = K$; (iii) $K \subset H$;
 - (iv) $H \not\subset K, K \not\subset H$.

Hint: Consider $G = \mathbb{Z}_n$.

- (b) Show that the submodule K in (a) above has the structure of a vector space over \mathbb{Z}_2 . Find $\dim K$ where $G = \mathbb{Z}_n$.
6. (a) Let q_1 and q_2 be rational numbers. Show that the set $\langle q_1, q_2 \rangle$ of all rationals of the form $m_1 q_1 + m_2 q_2$ ($m_1, m_2 \in \mathbb{Z}$) is a submodule of the \mathbb{Z} -module $(\mathbb{Q}, +)$ of all rational numbers.
- (b) Using the above notation show $1/6 \in \langle 3/2, 2/3 \rangle$. Show that $\langle 1/6 \rangle = \langle 3/2, 2/3 \rangle$.
- (c) Write $q_i = a_i/b_i \neq 0$ where $a_i, b_i \in \mathbb{Z}$, $\gcd\{a_i, b_i\} = 1$, $b_i > 0$ for $i = 1, 2$. Let $a'_i = a_i/\gcd\{a_1, a_2\}$, $b'_i = b_i/\gcd\{b_1, b_2\}$. Show that $\gcd\{a'_1 b'_2, a'_2 b'_1\} = 1$ and deduce $q_0 = \gcd\{a_1, a_2\}/\text{lcm}\{b_1, b_2\} \in \langle q_1, q_2 \rangle$. Conclude that q_0 generates $\langle q_1, q_2 \rangle$.
Hint: Remember $\text{lcm}\{b_1, b_2\} = b_1 b_2 / \gcd\{b_1, b_2\}$ and $\gcd\{a, b\} = \gcd\{a, c\} = 1 \Rightarrow \gcd\{a, bc\} = 1$ for $a, b, c \in \mathbb{Z}$.
 Is $\langle q_1, q_2, q_3 \rangle = \{m_1 q_1 + m_2 q_2 + m_3 q_3 : m_1, m_2, m_3 \in \mathbb{Z}\}$, where $q_1, q_2, q_3 \in \mathbb{Q}$, necessarily a cyclic submodule of \mathbb{Q} ?
- (d) Find a generator of $\langle 6/35, 75/56 \rangle$ and a generator of $\langle 6/35, 75/56, 8/15 \rangle$. Do either of these submodules contain \mathbb{Z} ?
7. (a) Let H_1 and H_2 be subgroups of the additive abelian group G . Show
 (i) the intersection $H_1 \cap H_2$ is a subgroup of G ,
 (ii) the sum $H_1 + H_2 = \{h_1 + h_2 : h_1 \in H_1, h_2 \in H_2\}$ is a subgroup of G ,
 (iii) the union $H_1 \cup H_2$ is a subgroup of $G \Leftrightarrow$ either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.
Hint: Show \Rightarrow by contradiction.
- (b) Find generators of $H_1 \cap H_2$ and $H_1 + H_2$ in the case of $G = \mathbb{Z}$, $H_1 = \langle 30 \rangle$, $H_2 = \langle 100 \rangle$. Generalise your answer to cover the case $G = \mathbb{Z}$, $H_1 = \langle m_1 \rangle$, $H_2 = \langle m_2 \rangle$.
8. (a) Let g_1, g_2, \dots, g_n ($n \geq 3$) be elements of an additive group G . The elements s_i of G are defined inductively by $s_1 = g_1$, $s_2 = s_1 + g_2$, $s_3 = s_2 + g_3$, \dots , $s_n = s_{n-1} + g_n$ ($1 \leq i \leq n$). Use the associative law of addition and induction to show that all ways of summing g_1, g_2, \dots, g_n in order give s_n .
Hint: Show first that each summation of g_1, g_2, \dots, g_n decomposes as $s_i + s'_{n-i}$ where s'_{n-i} is a summation of $g_{i+1}, g_{i+2}, \dots, g_n$ for some i with $1 \leq i < n$.
 Deduce the generalised associative law of addition: brackets may be omitted in any sum of n elements of G .
- (b) Let g_1, g_2, \dots, g_n ($n \geq 2$) be elements of an additive abelian group G . Use the associative and commutative laws of addition, and induction, to show that all ways of summing g_1, g_2, \dots, g_n in any order give s_n as defined in (a) above.

- (c) Let g, g_1, g_2 be elements of an additive abelian group G . Use (b) above to verify laws 5 and 6 of a \mathbb{Z} -module namely: $m(g_1 + g_2) = mg_1 + mg_2$, $(m_1 + m_2)g = m_1g + m_2g$, $(m_1m_2)g = m_1(m_2g)$ for all integers m, m_1, m_2 .

Hint: Suppose first that m, m_1, m_2 are positive.

2.2 Quotient Groups and the Direct Sum Construction

Two ways of obtaining new abelian groups from old are discussed: the *quotient group* construction and the *direct sum* construction. Particular cases of both constructions are already known to the reader, the most significant being \mathbb{Z}_n which is the quotient of \mathbb{Z} by its subgroup $\langle n \rangle$, that is, $\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$ for all positive integers n . Keep this familiar example in mind as the theory unfolds.

Let G be an additive abelian group having a subgroup K . We construct the quotient group G/K which can be thought of informally as G modulo K . Formally the elements of G/K are subsets of G of the type

$$K + g_0 = \{k + g_0 : k \in K\} \quad \text{for } g_0 \in G.$$

Subsets of this kind are called *cosets of K in G* . The elements of $K + g_0$ are sums $k + g_0$ where k runs through K and g_0 is a given element of G . We write $\overline{g_0} = K + g_0$ to emphasise the close analogy between cosets and congruence classes of integers. Notice that $g \in \overline{g_0}$ means $g = k + g_0$ for some $k \in K$, that is, $g - g_0 \in K$ showing that g differs from g_0 by an element of K . The condition $g - g_0 \in K$ is expressed by writing $g \equiv g_0 \pmod{K}$ and saying that g is *congruent* to g_0 modulo K . Our next lemma deals with the set-theoretic properties of cosets. Notice that each coset has as many aliases (alternative names) as it has elements!

Lemma 2.9

Let K be a subgroup of the additive abelian group G . Using the above notation $\overline{g} = \overline{g_0}$ if and only if $g \equiv g_0 \pmod{K}$. Congruence modulo K is an equivalence relation on G . Each element of G belongs to exactly one coset of K in G .

Proof

The subgroup K contains the zero element 0 of G . Hence $g = 0 + g \in \overline{g}$, showing that each g in G belongs to the coset \overline{g} . Suppose $\overline{g} = \overline{g_0}$ which means that the sets \overline{g} and $\overline{g_0}$ consist of exactly the same elements. As $g \in \overline{g}$ we see $g \in \overline{g_0}$ and so, as above, we conclude that $g \equiv g_0 \pmod{K}$.

Now suppose $g \equiv g_0 \pmod{K}$. Then $g - g_0 = k_0 \in K$. We first show $\bar{g} \subseteq \bar{g}_0$. Consider $x \in \bar{g}$. Then $x = k + g$ for $k \in K$. Hence $x = k + k_0 + g_0$ which belongs to \bar{g}_0 since $k + k_0 \in K$ as K is closed under addition. So we have shown $\bar{g} \subseteq \bar{g}_0$. Now K is closed under negation and so $g_0 - g = -k_0 \in K$ showing $g_0 \equiv g \pmod{K}$. Interchanging the roles of g and g_0 in the argument, we see that $\bar{g}_0 \subseteq \bar{g}$. The sets \bar{g} and \bar{g}_0 are such that each is a subset of the other, that is, $\bar{g} = \bar{g}_0$.

We now use the ‘if and only if’ condition $\bar{g} = \bar{g}_0 \Leftrightarrow g \equiv g_0 \pmod{K}$ to prove that congruence modulo K satisfies the three laws of an equivalence relation. As $\bar{g} = \bar{g}$ we see that $g \equiv g \pmod{K}$ for all $g \in G$, that is, congruence modulo K is reflexive. Suppose $g_1 \equiv g_2 \pmod{K}$ for some $g_1, g_2 \in G$; then $\bar{g}_1 = \bar{g}_2$ and so $\bar{g}_2 = \bar{g}_1$ which means $g_2 \equiv g_1 \pmod{K}$, that is, congruence modulo K is symmetric. Suppose $g_1 \equiv g_2 \pmod{K}$ and $g_2 \equiv g_3 \pmod{K}$ where $g_1, g_2, g_3 \in G$; then $\bar{g}_1 = \bar{g}_2$ and $\bar{g}_2 = \bar{g}_3$ and so $\bar{g}_1 = \bar{g}_3$ (it really is that easy!) which gives $g_1 \equiv g_3 \pmod{K}$, that is, congruence modulo K is transitive. Congruence modulo K satisfies the reflexive, symmetric and transitive laws and so is an equivalence relation on G .

The proof is finished by showing that no element g in G can belong to two different cosets of K in G . We know $g \in \bar{g}$ as $0 \in K$. Suppose $g \in \bar{g}_0$ for some $g_0 \in G$. The preliminary discussion shows $g \equiv g_0 \pmod{K}$ and hence $\bar{g} = \bar{g}_0$. So g belongs to \bar{g} and to no other coset of K in G . \square

The cosets of K in G *partition* the set G , that is, these cosets are non-empty, non-overlapping subsets having G as their union. In other words, each element of G belongs to a *unique* coset of K in G .

For example, let $G = \mathbb{Z}$ and $K = \langle 3 \rangle$. Then $m \equiv m' \pmod{K}$ means $m \equiv m' \pmod{3}$ for $m, m' \in \mathbb{Z}$. There are three cosets of K in G , namely $\bar{0} = K + 0 = K = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$, $\bar{1} = K + 1 = \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\}$, $\bar{2} = K + 2 = \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\}$ that is, the congruence classes of integers modulo 3 and these cosets partition \mathbb{Z} . So $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\} = G/K$ in this case.

Now suppose $G = \mathbb{Z}_{12}$ and $K = \langle \bar{4} \rangle$. There are four cosets of K in G and these are $K + \bar{0} = K = \{\bar{0}, \bar{4}, \bar{8}\}$, $K + \bar{1} = \{\bar{1}, \bar{5}, \bar{9}\}$, $K + \bar{2} = \{\bar{2}, \bar{6}, \bar{10}\}$, $K + \bar{3} = \{\bar{3}, \bar{7}, \bar{11}\}$.

These cosets partition \mathbb{Z}_{12} and we will see shortly that they are the elements of a cyclic group of order 4.

The number $|G/K|$ of cosets of K in G is called *the index* of the subgroup K in its parent group G . The index is either a positive integer or infinite. Let G be a *finite* abelian group, that is, the number $|G|$ of elements in G is a positive integer. In this case $|G|$ is called *the order* of G . The index of the subgroup K in G is the positive integer $|G/K|$. Every coset $K + g_0$ has exactly $|K|$ elements. As these $|G/K|$ cosets partition G , we obtain the equation $|G| = |G/K||K|$ and so

$$|G/K| = |G|/|K|$$

on counting the elements in G coset by coset. So $|K|$ is a divisor of $|G|$, that is,

the order $|K|$ of every subgroup K of a finite abelian group G is a divisor
of the order $|G|$ of G

which is known as *Lagrange's theorem* for finite abelian groups.

Each element g of G generates a cyclic subgroup $\langle g \rangle$. Suppose again that G is finite. Writing $K = \langle g \rangle$, from Theorem 2.5 we see that g has finite order $|K|$, and so $|K|g = 0$. Hence $|G|g = |G/K||K|g = |G/K| \times 0 = 0$. We have proved:

$|G|g = 0$ for all elements g of the finite abelian group G .

We call this useful fact the $|G|$ -*lemma*. For instance every element g of an additive abelian group of order 27 satisfies $27g = 0$. For each prime p the multiplicative group \mathbb{Z}_p^* is abelian of order $p - 1$, and so using multiplicative notation for a moment we obtain $(\bar{r})^{p-1} = \bar{1}$ for all $\bar{r} \in \mathbb{Z}_p^*$, that is, $r^{p-1} \equiv 1 \pmod{p}$ for all integers r and primes p with $\gcd\{r, p\} = 1$. On multiplying through by r we get

$$r^p \equiv r \pmod{p} \text{ for all integers } r \text{ and primes } p$$

which is known as *Fermat's 'little' theorem*.

Returning to the general case of an additive abelian group G with subgroup K , let $\eta : G \rightarrow G/K$ be the *natural mapping* defined by $(g)\eta = \bar{g}$ for all $g \in G$. So η maps each element g to the coset \bar{g} . Each coset of K in G is of the form \bar{g} for some $g \in G$ and so η is surjective. Can addition of cosets be introduced in such a way that G/K is an abelian group and η is an additive mapping as in Definition 2.3? There is only one possible way in which this can be done, because $(g_1 + g_2)\eta = (g_1)\eta + (g_2)\eta$, that is,

$$\overline{g_1 + g_2} = \bar{g}_1 + \bar{g}_2 \quad (\clubsuit)$$

tells us that the sum $\bar{g}_1 + \bar{g}_2$ of cosets must be the coset containing $g_1 + g_2$. The following lemma assures us that this rule of coset addition is unambiguous: it does not depend on the particular aliases used for \bar{g}_1 and \bar{g}_2 , and it does the job of turning the set G/K into an abelian group.

Lemma 2.10

Let G be an additive abelian group with subgroup K . Let g_1, g'_1, g_2, g'_2 be elements of G such that $g_1 \equiv g'_1 \pmod{K}$, $g_2 \equiv g'_2 \pmod{K}$. Then $g_1 + g_2 \equiv g'_1 + g'_2 \pmod{K}$. The above rule () of coset addition is unambiguous and G/K , with this addition, is an abelian group.

Proof

By hypothesis there are k_1, k_2 in K with $g_1 = k_1 + g'_1$, $g_2 = k_2 + g'_2$. Adding these equations and rearranging the terms, which is allowed as G is abelian, we obtain $g_1 + g_2 = (k_1 + g'_1) + (k_2 + g'_2) = (k_1 + k_2) + (g'_1 + g'_2)$ showing that $g_1 + g_2 \equiv g'_1 + g'_2 \pmod{K}$ as $k_1 + k_2 \in K$. So it is legitimate to add congruences modulo K . In terms of cosets, starting with $\overline{g_1} = \overline{g'_1}$, $\overline{g_2} = \overline{g'_2}$, we have shown $\overline{g_1 + g_2} = \overline{g'_1 + g'_2}$. Therefore coset addition is indeed unambiguously defined by

$$\overline{g_1} + \overline{g_2} = \overline{g_1 + g_2} \quad \text{for all } g_1, g_2 \in G$$

as the right-hand side is unchanged when the representatives of the cosets on the left-hand side are changed from g_i to g'_i , $i = 1, 2$.

We now verify that coset addition satisfies the laws of an abelian group. The associative law is satisfied as

$$\begin{aligned} (\overline{g_1} + \overline{g_2}) + \overline{g_3} &= \overline{(g_1 + g_2)} + \overline{g_3} = \overline{(g_1 + g_2) + g_3} \\ &= \overline{g_1 + (g_2 + g_3)} = \overline{g_1} + \overline{(g_2 + g_3)} = \overline{g_1} + (\overline{g_2} + \overline{g_3}) \end{aligned}$$

for all $g_1, g_2, g_3 \in G$. The coset $\overline{0} = \{k + 0 : k \in K\} = \{k : k \in K\} = K$ is the zero element of G/K since $\overline{0} + \overline{g} = \overline{0 + g} = \overline{g}$ for all $g \in G$. The coset \overline{g} has negative $\overline{-g}$ since $\overline{-g} + \overline{g} = \overline{-g + g} = \overline{0}$ and so $\overline{-g_1} = \overline{(-g_1)}$ for all $g \in G$. Finally, the commutative law holds in G/K since $\overline{g_1} + \overline{g_2} = \overline{g_1 + g_2} = \overline{g_2 + g_1} = \overline{g_2} + \overline{g_1}$ for all $g_1, g_2 \in G$. \square

The group G/K is called the *quotient* (or *factor*) *group* of G by K and $\eta : G \rightarrow G/K$ is called the *natural homomorphism*.

The additive group \mathbb{R} of real numbers contains the subgroup \mathbb{Z} of integers. A typical element of \mathbb{R}/\mathbb{Z} is the coset $\overline{x} = \{\dots, x - 2, x - 1, x, x + 1, x + 2, \dots\}$ consisting of all those numbers which differ from the real number x by an integer. For instance $\overline{1/3} = \{\dots, -5/3, -2/3, 1/3, 4/3, 7/3, \dots\}$. Every x is uniquely expressible $x = [x] + r$ where $[x]$ is an integer called the *integer part* of x , and r is a real number called the *fractional part* of x with $0 \leq r < 1$. For instance $[\pi] = 3$ and $\pi - [\pi] = 0.14159\dots$. In the group \mathbb{R}/\mathbb{Z} the integer part plays no role, but the fractional part is all-important as $\overline{x} = \overline{y}$ if and only if x and y have the same fractional part. So every element of \mathbb{R}/\mathbb{Z} can be expressed uniquely as \overline{r} where $0 \leq r < 1$. Suppose $0 \leq r_1, r_2 < 1$. Then coset addition in terms of fractional parts is given by

$$\overline{r_1} + \overline{r_2} = \begin{cases} \overline{r_1 + r_2} & \text{for } r_1 + r_2 < 1 \\ \overline{r_1 + r_2 - 1} & \text{for } r_1 + r_2 \geq 1. \end{cases}$$

For instance $\overline{1/2} + \overline{2/3} = \overline{1/6}$. The group \mathbb{R}/\mathbb{Z} is known as the *reals mod one* and we'll see in Section 2.3 that it's isomorphic to the multiplicative group of complex numbers of modulus 1.

The reader knows already that the additive group \mathbb{Z}_n is the particular case of the above construction with $G = \mathbb{Z}$, $K = \langle n \rangle$, that is, $\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$ is the standard example of a cyclic group of type C_n as defined in Definition 2.6 for $n \geq 0$. Note that $\mathbb{Z}_0 \cong \mathbb{Z}$ as the elements of \mathbb{Z}_0 are singletons (sets with exactly one element) $\{m\}$ for $m \in \mathbb{Z}$ and $\{m\} \rightarrow m$ is an isomorphism. At the other end of the scale the singleton $\mathbb{Z}_1 = \{\mathbb{Z}\}$ is the standard example of a trivial abelian group. Both \mathbb{Z} and its subgroups $\langle n \rangle$ are examples of *free* \mathbb{Z} -modules, that is, \mathbb{Z} -modules having \mathbb{Z} -bases. This concept will be discussed in Section 2.3. For the moment let's note that \mathbb{Z} has \mathbb{Z} -basis 1 (or -1) and $\langle n \rangle$ has \mathbb{Z} -basis n (or $-n$) for $n > 0$; the trivial \mathbb{Z} -module $\{0\}$ has \mathbb{Z} -basis the empty set \emptyset . The equation $\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$ expresses the additive group of \mathbb{Z}_n as a quotient of \mathbb{Z} (which is free) by its subgroup $\langle n \rangle$ (which is also free). It turns out that all f.g. abelian groups are best thought of as quotients of free \mathbb{Z} -modules by free subgroups, as we'll see in Section 3.1.

We now discuss the direct sum construction. You will be used to the formula $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$ for the sum of vectors. Carrying out addition in this componentwise way is the distinguishing feature of a direct sum.

Let G_1 and G_2 be additive abelian groups. The elements of $G_1 \oplus G_2$ are ordered pairs (g_1, g_2) where $g_1 \in G_1$, $g_2 \in G_2$. The rule of addition in $G_1 \oplus G_2$ is

$$(g_1, g_2) + (g'_1, g'_2) = (g_1 + g'_1, g_2 + g'_2) \quad \text{for } g_1, g'_1 \in G_1 \text{ and } g_2, g'_2 \in G_2.$$

It is straightforward to show that $G_1 \oplus G_2$ is itself an additive abelian group, and we confidently leave this job to the reader (Exercises 2.2, Question 4(f)). Suffice it to say that $(0_1, 0_2)$ is the zero element of $G_1 \oplus G_2$ where 0_i is the zero of G_i for $i = 1, 2$ and $-(g_1, g_2) = (-g_1, -g_2)$ showing that negation, like addition, is carried out component by component. The abelian group $G_1 \oplus G_2$ is called *the external direct sum* of G_1 and G_2 .

This construction, which is easier to grasp than the quotient group construction, produces 'at a stroke' a vast number of abelian groups. For instance

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2, \quad \mathbb{Z}_3 \oplus \mathbb{Z}, \quad (\mathbb{Z}_1 \oplus \mathbb{Z}_5) \oplus \mathbb{Z}, \quad (\mathbb{Z}_2 \oplus \mathbb{Z}_4) \oplus (\mathbb{Z}_4 \oplus \mathbb{Z}_7)$$

these groups being built up using cyclic groups and the direct sum construction. It turns out that all groups constructed in this way are abelian and finitely generated. Can *every* finitely generated abelian group be built up in this way? We will see in the next chapter that the answer is: Yes! What is more, the Smith normal form will help us decide which pairs of these groups are isomorphic.

We now look in detail at the group $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Write $0 = (\bar{0}, \bar{0})$, $u = (\bar{1}, \bar{0})$,

$v = (\bar{0}, \bar{1})$, $w = (\bar{1}, \bar{1})$. Then $G = \{0, u, v, w\}$ has addition table

| $+$ | 0 | u | v | w |
|-----|-----|-----|-----|-----|
| 0 | 0 | u | v | w |
| u | u | 0 | w | v |
| v | v | w | 0 | u |
| w | w | v | u | 0 |

Notice that the sum of any two of u, v, w is the other one, $v + w = u$ etc., and each element is equal to its negative, as $v + v = 0$ means $v = -v$ for instance. This group has five subgroups namely $\langle 0 \rangle$, $\langle u \rangle$, $\langle v \rangle$, $\langle w \rangle$ and G itself. Now G is not cyclic and we write $G = \langle u, v \rangle$ meaning that each element of G is of the form $lu + mv$ for some integers l and m . In fact G is the smallest non-cyclic group. Any group isomorphic to G is called a *Klein 4-group* after the German mathematician Felix Klein. Being the direct sum of two cyclic groups of order 2, G is said to be of *isomorphism type* $C_2 \oplus C_2$ (see Definition 2.13). You may have already met this group in the context of vector spaces because $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is the standard example of a 2-dimensional vector space over the field \mathbb{Z}_2 . The elements $0, u, v, w$ of G are the vectors and the elements $\bar{0}, \bar{1}$ of \mathbb{Z}_2 are the scalars. The ordered pair u, v is a basis of this vector space. The subgroups of G are precisely the subspaces and the automorphisms of G are precisely the invertible linear mappings θ of this vector space. For example $\theta : G \cong G$ such that $(0)\theta = 0$, $(u)\theta = v$, $(v)\theta = w$, $(w)\theta = u$ is an automorphism of G .

Using the approach outlined in the introduction, we now give the reader a glimpse ahead to Chapter 3. Just as the natural mapping $\eta : \mathbb{Z} \rightarrow \mathbb{Z}_2$ encapsulates the relationship between \mathbb{Z} and \mathbb{Z}_2 , so the \mathbb{Z} -linear mapping $\theta : \mathbb{Z} \oplus \mathbb{Z} \rightarrow G$, defined by $(l, m)\theta = lu + mv$ for all $l, m \in \mathbb{Z}$, tells us all there is to know about $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2$ in terms of the more tractable module $\mathbb{Z} \oplus \mathbb{Z}$; in fact $\mathbb{Z} \oplus \mathbb{Z}$ is a free \mathbb{Z} -module of *rank* 2 because $e_1 = (1, 0)$, $e_2 = (0, 1)$ is a \mathbb{Z} -basis having two ‘vectors’ (the term *rank* rather than *dimension* is used in this context). Note that $(e_1)\theta = 1u + 0v = u$ and similarly $(e_2)\theta = v$, $(e_1 + e_2)\theta = w$. So θ is surjective, that is, $\text{im } \theta = G$. Which pairs (l, m) of integers belong to the kernel of θ ? In other words, which pairs (l, m) of integers are mapped by θ to the zero element of G ? The answer is: l and m are both even, because this is the condition for the equation $lu + mv = 0$ to be true. So $\ker \theta = \langle 2e_1, 2e_2 \rangle$, that is, $\ker \theta$ consists of all integer linear combinations of $2e_1 = (2, 0)$ and $2e_2 = (0, 2)$. In fact $2e_1, 2e_2$ is a \mathbb{Z} -basis of $\ker \theta$ which is therefore a free subgroup of $\mathbb{Z} \oplus \mathbb{Z}$. Notice $2 = \text{rank } \ker \theta$. The \mathbb{Z} -bases of $\mathbb{Z} \oplus \mathbb{Z}$ and $\ker \theta$ are related by

$$D = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

We will see in Section 3.1 that f.g. abelian groups are not usually as prettily presented as this one; here the matrix D is already in Smith normal form. There are four cosets

of $K = \ker \theta$ in $\mathbb{Z} \oplus \mathbb{Z}$ depending on the parity of the integers l and m , that is,

$$(\mathbb{Z} \oplus \mathbb{Z})/K = \{K, K + e_1, K + e_2, K + e_1 + e_2\}$$

For instance, the elements of $K + e_1$ are the pairs (l, m) of integers with l odd, m even. These cosets correspond, using θ , to the elements $0, u, v, w$ respectively of $\text{im } \theta = G$, that is, $\tilde{\theta} : (\mathbb{Z} \oplus \mathbb{Z})/\ker \theta \cong G$ where

$$\begin{aligned} (K)\tilde{\theta} &= (0)\theta = 0, & (K + e_1)\tilde{\theta} &= (e_1)\theta = u, & (K + e_2)\tilde{\theta} &= (e_2)\theta = v, \\ (K + e_1 + e_2)\tilde{\theta} &= (e_1 + e_2)\theta = w. \end{aligned}$$

Kernels and images are defined at the start of Section 2.3. The isomorphism $\tilde{\theta}$, which is a particular case of Theorem 2.16, shows that the Klein 4-group is isomorphic to $(\mathbb{Z} \oplus \mathbb{Z})/\ker \theta$, a quotient of two free \mathbb{Z} -modules. The point is: every f.g. abelian group can be analysed in this way as we'll see in Theorem 3.4.

Frequently occurring examples of the direct sum construction are provided by the *Chinese remainder theorem*. This theorem which we now discuss plays an important role in the decomposition of rings and abelian groups. Let \bar{r}_n denote the congruence class of the integer r in \mathbb{Z}_n for all positive integers n . Let m and n be given positive integers and consider the mapping

$$\alpha : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n \quad \text{defined by } (\bar{r}_{mn})\alpha = (\bar{r}_m, \bar{r}_n) \quad \text{for all } \bar{r}_{mn} \in \mathbb{Z}_{mn}.$$

For instance with $m = 5$, $n = 7$ and $r = 24$ we have $(\overline{24})\alpha = (\bar{4}, \bar{3})$ since $24 \equiv 4 \pmod{5}$ and $24 \equiv 3 \pmod{7}$. Then α is unambiguously defined and respects addition since

$$\begin{aligned} (\bar{s}_{mn} + \bar{t}_{mn})\alpha &= ((\overline{s+t})_{mn})\alpha = ((\overline{s+t})_m, (\overline{s+t})_n) = (\bar{s}_m + \bar{t}_m, \bar{s}_n + \bar{t}_n) \\ &= (\bar{s}_m, \bar{s}_n) + (\bar{t}_m, \bar{t}_n) = (\bar{s}_{mn})\alpha + (\bar{t}_{mn})\alpha \quad \text{for all integers } s, t. \end{aligned}$$

The group $\mathbb{Z}_m \oplus \mathbb{Z}_n$ becomes a commutative ring (the direct sum of the rings \mathbb{Z}_m and \mathbb{Z}_n) provided multiplication is carried out, like addition, component by component, that is, $(x, y)(x', y') = (xx', yy')$ for all $x, x' \in \mathbb{Z}_m$ and $y, y' \in \mathbb{Z}_n$. Replacing each '+' in the above equations by the product symbol ' \cdot ' produces

$$(\bar{s}_{mn} \cdot \bar{t}_{mn})\alpha = (\bar{s}_{mn})\alpha \cdot (\bar{t}_{mn})\alpha \quad \text{for all integers } s, t$$

showing that α respects multiplication. Also $\bar{1}_{mn}$ is the 1-element of \mathbb{Z}_{mn} and $(\bar{1}_{mn})\alpha = (\bar{1}_m, \bar{1}_n)$ is the 1-element of $\mathbb{Z}_m \oplus \mathbb{Z}_n$. Therefore

$$\alpha \text{ is a ring homomorphism}$$

meaning that α is a mapping of rings which respects addition, multiplication and 1-elements.

Theorem 2.11 (The Chinese remainder theorem)

Let m and n be positive integers with $\gcd\{m, n\} = 1$. Then $\alpha : \mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$ is a ring isomorphism.

Proof

Using the above theory, α is a ring homomorphism and so it is enough to show that α is bijective. As \mathbb{Z}_{mn} and $\mathbb{Z}_m \oplus \mathbb{Z}_n$ both contain exactly mn elements it is enough to show that α is surjective. Consider a typical element (\bar{s}_m, \bar{t}_n) of $\mathbb{Z}_m \oplus \mathbb{Z}_n$. We may assume $0 \leq s < m$ and $0 \leq t < n$. Can an integer r be found which leaves remainder s on division by m and remainder t on division by n ? (Special cases of this problem were solved in ancient China – hence the name of the theorem.) The answer is: Yes! Let $r = atm + bsn$ where a, b are integers with $am + bn = 1$. Then $r \equiv bsn \pmod{m}$ and $bsn = s - sam \equiv s \pmod{m}$. So $r \equiv s \pmod{m}$. Similarly $r \equiv t \pmod{n}$ and so r leaves remainders s, t on division by m, n respectively. Therefore $(\bar{r}_{mn})\alpha = (\bar{r}_m, \bar{r}_n) = (\bar{s}_m, \bar{t}_n)$ showing that α is indeed surjective. \square

Let R be a ring with 1-element e . An element u of R is a *unit* (invertible element) of R if there is an element v of R with $uv = e = vu$. It is straightforward to verify that the product uu' of units of R is itself a unit of R , and together with this product the set of units of R is a multiplicative group $U(R)$. Note that $U(F) = F^*$ for every field F , as every non-zero element of F is a unit of F . The groups $U(\mathbb{Z}_n)$ are studied in Section 3.3. We now use Theorem 2.11 to determine the order $|U(\mathbb{Z}_n)|$ of $U(\mathbb{Z}_n)$ in terms of the prime factorisation of the positive integer n . The reader will know that \bar{r} is a unit of \mathbb{Z}_n if and only if $\gcd\{r, n\} = 1$. It is convenient to assume (as we may) that $1 \leq r \leq n$. The reader may also have met the *Euler ϕ -function* defined by

$$\phi(n) = |\{r : 1 \leq r \leq n, \gcd\{r, n\} = 1\}|$$

that is, $\phi(n)$ is the *number* of integers r between 1 and n which are coprime to the positive integer n , and so $\phi(n) = |U(\mathbb{Z}_n)|$. One sees directly that $\phi(1) = 1$ and $\phi(p) = p - 1$ for all primes p . The closed interval $[1, p^l]$ contains p^l integers and the p^{l-1} multiples of p in this interval are exactly those which are *not* coprime to p since $\gcd\{r, p^l\} \neq 1 \Leftrightarrow p|r$; hence $\phi(p^l) = p^l - p^{l-1}$. In particular $\phi(7) = 7 - 1 = 6$, $\phi(8) = 8 - 4 = 4$, $\phi(9) = 9 - 3 = 6$.

Corollary 2.12

The Euler ϕ -function is multiplicative, that is, $\phi(mn) = \phi(m)\phi(n)$ where m, n are coprime positive integers. Let $n = p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}$ where p_1, p_2, \dots, p_k are different primes. Then $\phi(n) = (p_1^{l_1} - p_1^{l_1-1})(p_2^{l_2} - p_2^{l_2-1}) \cdots (p_k^{l_k} - p_k^{l_k-1})$.

Proof

As multiplication in $\mathbb{Z}_m \oplus \mathbb{Z}_n$ is carried out componentwise, (\bar{s}_m, \bar{t}_n) is a unit of the ring $\mathbb{Z}_m \oplus \mathbb{Z}_n$ if and only if \bar{s}_m is a unit of the ring \mathbb{Z}_m and \bar{t}_n is a unit of the ring \mathbb{Z}_n . Therefore $U(\mathbb{Z}_m \oplus \mathbb{Z}_n) = U(\mathbb{Z}_m) \times U(\mathbb{Z}_n)$ where \times denotes the Cartesian product (see Exercises 2.3, Question 4(d)). Comparing sizes of these sets gives $|U(\mathbb{Z}_m \oplus \mathbb{Z}_n)| = |U(\mathbb{Z}_m)||U(\mathbb{Z}_n)| = \phi(m)\phi(n)$. Suppose $\gcd\{m, n\} = 1$. As isomorphic rings have isomorphic groups of units, or specifically in our case, \bar{r}_{mn} is a unit of \mathbb{Z}_{mn} if and only if $(\bar{r}_{mn})\alpha$ is a unit of $\mathbb{Z}_m \oplus \mathbb{Z}_n$ by Theorem 2.11, we deduce $\phi(mn) = |U(\mathbb{Z}_{mn})| = |U(\mathbb{Z}_m \oplus \mathbb{Z}_n)|$. So $\phi(mn) = \phi(m)\phi(n)$ where $\gcd\{m, n\} = 1$.

We use induction on the number k of distinct prime divisors of n . As $\phi(1) = 1$ we take $k > 0$ and assume $\phi(p_2^{l_2} \cdots p_k^{l_k}) = (p_2^{l_2} - p_2^{l_2-1}) \cdots (p_k^{l_k} - p_k^{l_k-1})$. As $\gcd\{p_1^{l_1}, p_2^{l_2}, \dots, p_k^{l_k}\} = 1$, the multiplicative property of ϕ gives

$$\begin{aligned} \phi(n) &= \phi(p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}) = \phi(p_1^{l_1}) \phi(p_2^{l_2} \cdots p_k^{l_k}) \\ &= (p_1^{l_1} - p_1^{l_1-1})(p_2^{l_2} - p_2^{l_2-1}) \cdots (p_k^{l_k} - p_k^{l_k-1}) \end{aligned}$$

as in Corollary 2.12. By induction, the formula for $\phi(n)$ is as stated. \square

For example $\phi(500) = \phi(2^2 5^3) = \phi(2^2) \phi(5^3) = (2^2 - 2)(5^3 - 5^2) = 200$.

Let n be a positive integer. Which elements $\bar{r} \in \mathbb{Z}_n$ satisfy $\langle \bar{r} \rangle = \mathbb{Z}_n$? In other words, which elements of the additive abelian group \mathbb{Z}_n have order n ? We may assume $1 \leq r \leq n$. As $\bar{1}_n$ has order n and $\bar{r} = r\bar{1}_n$, by Lemma 2.7 we see that \bar{r} has order $n/\gcd\{r, n\}$. So \bar{r} has order n if and only if $\gcd\{r, n\} = 1$. Hence

each finite cyclic group of order n has $\phi(n)$ generators.

For instance \mathbb{Z}_{10} has $\phi(10) = (2 - 1)(5 - 1) = 4$ generators and $\mathbb{Z}_{10} = \langle \bar{1} \rangle = \langle \bar{3} \rangle = \langle \bar{7} \rangle = \langle \bar{9} \rangle$.

The direct sum construction can be extended to any finite number t of \mathbb{Z} -modules. Let G_1, G_2, \dots, G_t be \mathbb{Z} -modules. Their *external direct sum* $G_1 \oplus G_2 \oplus \cdots \oplus G_t$ is the \mathbb{Z} -module having all ordered t -tuples (g_1, g_2, \dots, g_t) where $g_i \in G_i$ ($1 \leq i \leq t$) as its elements, addition and integer multiplication being carried out componentwise. So $(g_1, g_2, \dots, g_t) + (g'_1, g'_2, \dots, g'_t) = (g_1 + g'_1, g_2 + g'_2, \dots, g_t + g'_t)$ for $g_i, g'_i \in G_i$ and $m(g_1, g_2, \dots, g_t) = (mg_1, mg_2, \dots, mg_t)$ for $m \in \mathbb{Z}$, $g_i \in G_i$ where $1 \leq i \leq t$.

We now generalise Definition 2.6.

Definition 2.13

Suppose the \mathbb{Z} -module G_i is cyclic of isomorphism type C_{d_i} for $1 \leq i \leq t$. Any \mathbb{Z} -module G isomorphic to $G_1 \oplus G_2 \oplus \cdots \oplus G_t$ is said to be of *isomorphism type* $C_{d_1} \oplus C_{d_2} \oplus \cdots \oplus C_{d_t}$.

For instance the additive group G of the ring $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ has isomorphism type $C_2 \oplus C_3$. By Theorem 2.11 we know that G is cyclic of isomorphism type C_6 and so we write $C_2 \oplus C_3 = C_6$ since the isomorphism class of \mathbb{Z} -modules of type $C_2 \oplus C_3$ coincides with the isomorphism class of \mathbb{Z} -modules of type C_6 . Also $C_2 \oplus C_3 = C_3 \oplus C_2$ as $G_1 \oplus G_2 \cong G_2 \oplus G_1$ for all \mathbb{Z} -modules G_1 and G_2 . More generally for positive integers m and n we have

$$C_m \oplus C_n = C_n \oplus C_m \quad \text{and} \quad C_m \oplus C_n = C_{mn} \quad \text{in case } \gcd\{m, n\} = 1$$

by Theorem 2.11. We will use these rules in Chapter 3 to manipulate the isomorphism type symbols and show Theorem 3.4 that every finitely generated \mathbb{Z} -module G is of isomorphism type $C_{d_1} \oplus C_{d_2} \oplus \cdots \oplus C_{d_t}$ where the non-negative integers d_i are successive divisors, that is, $d_i | d_{i+1}$ for $1 \leq i < t$.

Next we generalise the Chinese remainder theorem. Using Theorem 2.11 and induction on k we obtain the ring isomorphism

$$\alpha : \mathbb{Z}_n \cong \mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_2} \oplus \cdots \oplus \mathbb{Z}_{q_k} \quad \text{given by } (r_n)\alpha = (r_{q_1}, r_{q_2}, \dots, r_{q_k})$$

for all $r \in \mathbb{Z}$, where $n = q_1 q_2 \cdots q_k$ and q_1, q_2, \dots, q_k are powers of distinct primes p_1, p_2, \dots, p_k . For example consider $\alpha : \mathbb{Z}_{60} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$. As 11 leaves remainders 3, 2, 1 on division by 4, 3, 5 respectively we see (suppressing the subscripts) that $(\overline{11})\alpha = (\overline{3}, \overline{2}, \overline{1})$. Doubling gives $(\overline{22})\alpha = (\overline{6}, \overline{4}, \overline{2}) = (\overline{2}, \overline{1}, \overline{2})$ and negating gives $(\overline{49})\alpha = (-\overline{11})\alpha = (-\overline{3}, -\overline{2}, -\overline{1}) = (\overline{1}, \overline{1}, \overline{4})$. Squaring gives $((\overline{22})^2)\alpha = (\overline{2}, \overline{1}, \overline{2})^2 = (\overline{2}^2, \overline{1}^2, \overline{2}^2) = (\overline{0}, \overline{1}, \overline{4}) = (\overline{4})\alpha$ and so $(\overline{22})^2 = \overline{4}$ in \mathbb{Z}_{60} . Similarly $((\overline{49})^2)\alpha = (\overline{1}, \overline{1}, \overline{1}) = (\overline{1})\alpha$ showing that $\overline{49}$ is a self-inverse element of \mathbb{Z}_{60} as $(\overline{49})^2 = \overline{1}$, that is, $(\overline{49})^{-1} = \overline{49}$ in \mathbb{Z}_{60} . It is an amazing fact that the 60 triples in $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$ add and multiply in exactly the same way as the 60 elements of \mathbb{Z}_{60} .

We now look at the direct sum construction from the opposite point of view. Under which circumstances is the \mathbb{Z} -module G isomorphic to a direct sum $G_1 \oplus G_2$ of \mathbb{Z} -modules? We will see shortly that the submodules of G hold the answer to this question. Let 0_i denote the zero element of the \mathbb{Z} -module G_i for $i = 1, 2$. Then $G_1 \oplus G_2$ has submodules $G'_1 = \{(g_1, 0_2) : g_1 \in G_1\}$ and $G'_2 = \{(0_1, g_2) : g_2 \in G_2\}$ which are isomorphic to G_1 and G_2 respectively. Also each element (g_1, g_2) of $G_1 \oplus G_2$ is *uniquely* expressible as a sum $g'_1 + g'_2$, where $g'_1 \in G'_1$, $g'_2 \in G'_2$, since $(g_1, g_2) = g'_1 + g'_2$ if and only if $g'_1 = (g_1, 0_2)$, $g'_2 = (0_1, g_2)$. Consider an isomorphism $\alpha : G \cong G_1 \oplus G_2$ and let $H_i = \{h_i \in G : (h_i)\alpha \in G'_i\}$ for $i = 1, 2$. So H_1 and H_2 are the submodules of G which correspond under α to G'_1 and G'_2 . We write

$$G = H_1 \oplus H_2 \quad \text{and call } G \text{ the internal direct sum of its submodules } H_1 \text{ and } H_2$$

as each element g of G is *uniquely* expressible as $g = h_1 + h_2$ where $h_1 \in H_1$ and $h_2 \in H_2$, since α is an isomorphism.

For example $\alpha : \mathbb{Z}_6 \rightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_3$ as above leads to the submodules $H_1 = \{\bar{0}, \bar{3}\}$ and $H_2 = \{\bar{0}, \bar{2}, \bar{4}\}$. The six elements of \mathbb{Z}_6 are

$$\bar{0} = \bar{0} + \bar{0}, \quad \bar{1} = \bar{3} + \bar{4}, \quad \bar{2} = \bar{0} + \bar{2}, \quad \bar{3} = \bar{3} + \bar{0}, \quad \bar{4} = \bar{0} + \bar{4}, \quad \bar{5} = \bar{3} + \bar{2}$$

and they coincide as shown with the six elements $h_1 + h_2$ where $h_1 \in H_1, h_2 \in H_2$. So $\mathbb{Z}_6 = H_1 \oplus H_2$ is the internal direct sum of its submodules H_1 and H_2 . Of course it is equally true that $\mathbb{Z}_6 = H_2 \oplus H_1$. More generally the order in which the H_i (the *summands*) appear in any internal direct sum is not important. The Klein 4-group $G = \{0, u, v, w\}$ can be *decomposed* (expressed as an internal direct sum) as

$$G = \langle u \rangle \oplus \langle v \rangle = \langle v \rangle \oplus \langle w \rangle = \langle w \rangle \oplus \langle u \rangle$$

which tells us (three times!) that G , being the internal direct sum of two cyclic subgroups of order 2, has isomorphism type $C_2 \oplus C_2$.

The argument of the paragraph above can be extended. Let G be a \mathbb{Z} -module with submodules H_1, H_2, \dots, H_t such that for each element g in G there are *unique* elements h_i in H_i ($1 \leq i \leq t$) with $g = h_1 + h_2 + \dots + h_t$. It is straightforward to check that $\alpha : G \cong H_1 \oplus H_2 \oplus \dots \oplus H_t$, defined by $(g)\alpha = (h_1, h_2, \dots, h_t)$, is an isomorphism; so G is isomorphic to the external direct sum of the \mathbb{Z} -modules H_1, H_2, \dots, H_t . Generalising the above paragraph it is usual to write $G = H_1 \oplus H_2 \oplus \dots \oplus H_t$ and call G the *internal direct sum* of its submodules H_1, H_2, \dots, H_t .

Confused? We've shown that the internal direct sum of the H_i , when it exists, is isomorphic to the external direct sum of the H_i . Nevertheless we'll usually tell the reader, when it occurs in the theory ahead, which version of direct sum we have in mind.

As we have already seen $\mathbb{Z}_6 = \langle \bar{3} \rangle \oplus \langle \bar{4} \rangle$ as \mathbb{Z}_6 is the internal direct sum of $H_1 = \langle \bar{3} \rangle$ and $H_2 = \langle \bar{4} \rangle$; note that $(\bar{3})\alpha = (\bar{1}, \bar{0})$ and $(\bar{4})\alpha = (\bar{0}, \bar{1})$. In the same way let us look at $\alpha : \mathbb{Z}_{60} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$. How can we quickly find \bar{r} in \mathbb{Z}_{60} with $(\bar{r})\alpha = (\bar{1}, \bar{0}, \bar{0})$ and $1 \leq r \leq 60$? As r is divisible by 3 and 5 there are only four possibilities: 15, 30, 45 and 60. So $r = 45$ as $r \equiv 1 \pmod{4}$. The reader can check that $(\bar{40})\alpha = (\bar{0}, \bar{1}, \bar{0})$, $(\bar{36})\alpha = (\bar{0}, \bar{0}, \bar{1})$. So $\mathbb{Z}_{60} = \langle \bar{45} \rangle \oplus \langle \bar{40} \rangle \oplus \langle \bar{36} \rangle$ shows how \mathbb{Z}_{60} decomposes as an internal direct sum.

Let H_1, H_2, \dots, H_t be submodules of the \mathbb{Z} -module G . It is straightforward to verify that their *sum*

$$H_1 + H_2 + \dots + H_t = \{h_1 + h_2 + \dots + h_t : h_i \in H_i \text{ for all } 1 \leq i \leq t\}$$

is a submodule of G . For example take $G = \mathbb{Z}_{60}$, $H_1 = \langle \bar{6} \rangle$, $H_2 = \langle \bar{10} \rangle$, $H_3 = \langle \bar{15} \rangle$. As $\bar{1} = \bar{6} + \bar{10} - \bar{15}$ and so $\bar{r} = \bar{6}r + \bar{10}r + (-\bar{15}r) \in H_1 + H_2 + H_3$ for $\bar{r} \in \mathbb{Z}_{60}$, we see $G = H_1 + H_2 + H_3$. However $\bar{1} = \bar{6} - \bar{2} \times \bar{10} + \bar{15}$ showing that $\bar{1}$ can be expressed in at least two ways as a sum $h_1 + h_2 + h_3$ with $h_i \in H_i$. Conclusion: G is *not* the internal direct sum of H_1, H_2 and H_3 as there's no such thing! The uniqueness condition of

the internal direct sum is violated. The next lemma tells us the best way of checking whether or not a sum of submodules is direct.

Definition 2.14

The submodules H_i ($1 \leq i \leq t$) of the \mathbb{Z} -module G are called *independent* if the equation $h_1 + h_2 + \cdots + h_t = 0$, where $h_i \in H_i$ for all i with $1 \leq i \leq t$, holds only in the case $h_1 = h_2 = \cdots = h_t = 0$.

The reader should note the similarity between Definition 2.14 and linear independence of vectors. We show next that the internal direct sum of independent submodules always exists.

Lemma 2.15

Let H_1, H_2, \dots, H_t be independent submodules of the \mathbb{Z} -module G such that $G = H_1 + H_2 + \cdots + H_t$. Then $G = H_1 \oplus H_2 \oplus \cdots \oplus H_t$.

Proof

Consider $g \in G$. As $G = H_1 + H_2 + \cdots + H_t$ there are $h_i \in H_i$ ($1 \leq i \leq t$) with $g = h_1 + h_2 + \cdots + h_t$. Suppose $g = h'_1 + h'_2 + \cdots + h'_t$ where $h'_i \in H_i$ ($1 \leq i \leq t$). Subtracting produces $0 = g - g = (h_1 - h'_1) + (h_2 - h'_2) + \cdots + (h_t - h'_t)$. As $h_i - h'_i \in H_i$ we deduce $h_i - h'_i = 0$ ($1 \leq i \leq t$) using the independence of H_1, H_2, \dots, H_t . Hence $h_i = h'_i$ for $1 \leq i \leq t$ showing that g is uniquely expressible as a sum of elements, one from each H_i . Therefore $G = H_1 \oplus H_2 \oplus \cdots \oplus H_t$. \square

Remember that the external direct sum $G_1 \oplus G_2$ makes sense for all \mathbb{Z} -modules G_1 and G_2 . But the internal direct sum of submodules exists only in the special case of *independent* submodules detailed above. Nevertheless we shall see in Chapter 3 that this special case frequently occurs.

EXERCISES 2.2

1. (a) Let $G = \mathbb{Z}_8$ and $K = \{\bar{0}, \bar{4}\}$. List the 4 cosets of K in G . Show that G/K is cyclic and state its isomorphism type.
- (b) Let $G = \mathbb{Z}_{12}$ and $K = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\} = \langle \bar{3} \rangle$. List the 3 cosets of K in G . Show that $K + \bar{1}$ generates G/K . State the isomorphism type of G/K .

- (c) Let $G = \mathbb{Z}_{24}$ and $K = \langle \overline{18} \rangle$. Show $|K| = 4$. What is the order of G/K ? Show that G/K is cyclic and state its isomorphism type.
- (d) Write $G = \mathbb{Z}_n$, $K = \langle \overline{m} \rangle$ where $\overline{m} \in \mathbb{Z}_n$. Use Lemma 2.7 to determine $|K|$ and $|G/K|$. Show that G/K is cyclic and state its isomorphism type.
2. (a) Let d be a positive divisor of the positive integer n . Use Lemma 2.2 to show that \mathbb{Z}_n has a unique subgroup K of index d .
- (b) Let d be a positive integer. Use Theorem 1.15 to show that \mathbb{Z} has a unique subgroup K of index d . Does every subgroup of \mathbb{Z} have finite index?
- (c) Let G be a cyclic group with subgroup K . Show that G/K is cyclic.
Hint: Use a generator of G to find a generator of G/K .
3. (a) Let \mathbb{Q} denote the additive group of rational numbers. In the group \mathbb{Q}/\mathbb{Z} of *rational mod one* find the orders of $\mathbb{Z} + 1/3$ and $\mathbb{Z} + 5/8$. Show that every element of \mathbb{Q}/\mathbb{Z} has finite order.
- (b) Let K be a subgroup of \mathbb{Q}/\mathbb{Z} and suppose $\mathbb{Z} + m/n, \mathbb{Z} + m'/n'$ belong to K where $\gcd\{m, n\} = 1$, $\gcd\{m', n'\} = 1$. Use integers a, b with $am + bn = 1$ to show that $\mathbb{Z} + 1/n \in K$. Show also $\mathbb{Z} + d/nn' \in K$ where $d = \gcd\{n, n'\}$. Suppose K is finite. Show that K is cyclic.
Hint: Consider $\mathbb{Z} + 1/n \in K$ with n maximum.
- (c) Let n be a positive integer. Show that \mathbb{Q}/\mathbb{Z} has a unique subgroup of order n .
Hint: Use (b) above.
- (d) Let $K = \{\mathbb{Z} + l/2^s : l, s \in \mathbb{Z}, s \geq 0\}$. Show that K is a subgroup of \mathbb{Q}/\mathbb{Z} having infinite order. List the finite subgroups of K . Show that K has a unique infinite subgroup. (The group K is denoted by $\mathbb{Z}(2^\infty)$.)
4. (a) Verify that $\mathbb{Z}_3 \oplus \mathbb{Z}_4$ has generator $g = (\overline{1}_3, \overline{1}_4)$ by listing the elements $g, 2g, 3g, 4g, \dots$ in the form $(\overline{s}, \overline{t})$ where $0 \leq s < 3, 0 \leq t < 4$. State its isomorphism type.
- (b) Find the orders of the 8 non-zero elements of $G = \mathbb{Z}_3 \oplus \mathbb{Z}_3$. Specify generators of the 4 subgroups of order 3. Express G in six ways as the internal direct sum of subgroups of order 3. State the isomorphism type of G .
Hint: G is a vector space over \mathbb{Z}_3 and the subgroups are subspaces.
- (c) Let the elements g_i of the \mathbb{Z} -module G_i have finite order n_i ($i = 1, 2$). Show that the element (g_1, g_2) of the external direct sum $G_1 \oplus G_2$ has order $l = \text{lcm}\{n_1, n_2\} = n_1 n_2 / \gcd\{n_1, n_2\}$.
Hint: Start by showing that (g_1, g_2) has finite order n say, where $n|l$. Then show $n_i|n$.
- (d) Let m and n be coprime positive integers. Use Lemma 2.7 and part (c) above to show that $(\overline{s}, \overline{t})$ in $\mathbb{Z}_m \oplus \mathbb{Z}_n$ has order mn if and only if

$\gcd\{s, m\} = 1$, $\gcd\{t, n\} = 1$. How many generators does the cyclic group $\mathbb{Z}_7 \oplus \mathbb{Z}_8$ have?

- (e) Let g and h be elements of an additive abelian group having orders m and n where $\gcd\{m, n\} = 1$. Show that $g + h$ has order mn .

The additive abelian group G has a cyclic subgroup K of order m such that G/K is cyclic of order n where $\gcd\{m, n\} = 1$. Show that G is cyclic of order mn .

Hint: Let $K + h_0$ generate G/K . Deduce from Exercises 2.1, Question 4(b) that n is a divisor of the order s of h_0 . Now use g and h where $\langle g \rangle = K$ and $h = (s/n)h_0$.

- (f) Let G_1 and G_2 be additive abelian groups. Show that their external direct sum $G_1 \oplus G_2$ is an additive abelian group. Show that $G_1 \oplus G_2$ and $G_2 \oplus G_1$ are isomorphic.
5. (a) Find \bar{r} in \mathbb{Z}_{143} such that r leaves remainders 7 and 6 on division by 11 and 13 respectively.
- (b) Find the 4 elements $x \in \mathbb{Z}_{143}$ satisfying $x^2 = x$.
Hint: First solve $x^2 = x$ for $x \in \mathbb{Z}_{11}$ and secondly for $x \in \mathbb{Z}_{13}$. Then use the Chinese remainder theorem.
- (c) Find the 4 elements $x \in \mathbb{Z}_{143}$ satisfying $x^2 = \bar{1}$, and the 9 elements $x \in \mathbb{Z}_{143}$ satisfying $x^3 = x$.
Hint: Use the method of (b) above.
- (d) How many \mathbb{Z} -linear mappings $\theta : \mathbb{Z}_3 \oplus \mathbb{Z}_5 \rightarrow \mathbb{Z}_{15}$ are there? How many of these mappings are (i) group isomorphisms, (ii) ring isomorphisms?
Hint: Consider $\bar{r} \in \mathbb{Z}_{15}$ where $(\bar{1}_3, \bar{1}_5)\theta = \bar{r}$.
6. (a) Let m_1, m_2, \dots, m_t be integers. Show

$$\mathbb{Z} = \langle m_1 \rangle + \langle m_2 \rangle + \cdots + \langle m_t \rangle \quad \Leftrightarrow \quad \gcd\{m_1, m_2, \dots, m_t\} = 1.$$

Is $\mathbb{Z} = \langle 15 \rangle + \langle 36 \rangle + \langle 243 \rangle$? Is $\mathbb{Z} = \langle 15 \rangle + \langle 36 \rangle + \langle 80 \rangle$?

- (b) Suppose $\mathbb{Z} = H_1 \oplus H_2$ (internal direct sum of subgroups). Use Theorem 1.15 to show that \mathbb{Z} is *indecomposable*, that is, either H_1 or H_2 is trivial.
- (c) Let H_1 and H_2 be submodules of the \mathbb{Z} -module G such that $H_1 \cap H_2 = \{0\}$. Show that H_1, H_2 are independent. More generally, let $H_1, H_2, \dots, H_{t-1}, H_t$ be submodules of G such that H_1, H_2, \dots, H_{t-1} are independent and $(H_1 + H_2 + \cdots + H_{t-1}) \cap H_t = \{0\}$. Show that $H_1, H_2, \dots, H_{t-1}, H_t$ are independent. What is the order of $H_1 \oplus H_2 \oplus \cdots \oplus H_t$ given that each H_i is finite?
- (d) Write $G = \mathbb{Z}_3 \oplus \mathbb{Z}_9$ (external direct sum of abelian groups). Use Question 4(d) above to show that G has 18 elements of order 9 and 8 elements of order 3. Deduce that G has 3 cyclic subgroups of order 9 and

4 cyclic subgroups of order 3. (Remember that a cyclic group of order n has $\phi(n)$ generators.) Specify generators of these 7 cyclic subgroups of G . Find the number of pairs of cyclic subgroups H_1, H_2 of G with $|H_1| = 3, |H_2| = 9$ such that $G = H_1 \oplus H_2$.

Hint: Choose H_2 first and then H_1 with $H_1 \cap H_2 = \{0\}$.

- (e) Let H_1, H_2, \dots, H_t be independent submodules of a \mathbb{Z} -module G and let K_i be a submodule of H_i for $1 \leq i \leq t$. Show that K_1, K_2, \dots, K_t are independent. Write

$$H = H_1 \oplus H_2 \oplus \cdots \oplus H_t \quad \text{and} \quad K = K_1 \oplus K_2 \oplus \cdots \oplus K_t$$

(internal direct sums). Show

$$H/K \cong (H_1/K_1) \oplus (H_2/K_2) \oplus \cdots \oplus (H_t/K_t)$$

(external direct sum).

Hint: Consider α defined by

$$(K + h)\alpha = (K_1 + h_1, K_2 + h_2, \dots, K_t + h_t)$$

where $h = h_1 + h_2 + \cdots + h_t, h_i \in H_i$ for $1 \leq i \leq t$. Show first that α is unambiguously defined.

2.3 The First Isomorphism Theorem and Free Modules

In this section we introduce the last two topics required for our onslaught on f.g. abelian groups. First we explain how each homomorphism of abelian groups gives rise to an isomorphism; this is the first isomorphism theorem and it plays a vital role in expressing every f.g. abelian group as a quotient group \mathbb{Z}^t/K , both \mathbb{Z}^t (the external direct sum of t copies of \mathbb{Z}) and its subgroup K being free \mathbb{Z} -modules. Secondly we discuss bases of free modules. Some of the theorems are analogous to those familiar to the reader in the context of finite-dimensional vector spaces – it's nice to know that two bases of the same free module are guaranteed to have the same number of elements (this number is called the *rank* of the free module and is analogous to *dimension* of a vector space). Also the rows of invertible $t \times t$ matrices over \mathbb{Z} are, as one might expect, precisely the \mathbb{Z} -bases of \mathbb{Z}^t . So far so good, but the analogy has its shortcomings. For example only certain \mathbb{Z} -independent subsets of \mathbb{Z}^t can be extended to \mathbb{Z} -bases of \mathbb{Z}^t (see Exercises 1.3, Question 5(c)). Dually, there are subsets of \mathbb{Z}^t which generate \mathbb{Z}^t but which don't contain a \mathbb{Z} -basis of \mathbb{Z}^t ; in fact $\{2, 3\}$ is such a subset of $\mathbb{Z} = \mathbb{Z}^1$ as $\langle 2, 3 \rangle = \mathbb{Z}$, $\langle 2 \rangle \neq \mathbb{Z}$, $\langle 3 \rangle \neq \mathbb{Z}$. The message is: take nothing for granted!

Let G and G' be \mathbb{Z} -modules and let $\theta : G \rightarrow G'$ be a \mathbb{Z} -linear mapping. As we've seen in previous discussions, there are two important submodules associated with θ . The first is the kernel of θ and consists of those elements of G which θ maps to the zero element $0'$ of G' . Therefore

$$\ker \theta = \{g \in G : (g)\theta = 0'\}$$

It is routine to show that $\ker \theta$ is a submodule of G .

The second is the image of θ and consists of those elements of G' which are images by θ of elements in G . Therefore

$$\operatorname{im} \theta = \{(g)\theta : g \in G\}$$

Again it is routine to show that $\operatorname{im} \theta$ is a submodule of G' (see Exercises 2.3, Question 1(a)).

Next we show how θ gives rise to an isomorphism $\tilde{\theta}$.

Theorem 2.16 (The first isomorphism theorem for \mathbb{Z} -modules)

Let G and G' be \mathbb{Z} -modules and let $\theta : G \rightarrow G'$ be a \mathbb{Z} -linear mapping. Write $K = \ker \theta$. Then $\tilde{\theta}$, defined by $(K + g)\tilde{\theta} = (g)\theta$ for all $g \in G$, is an isomorphism

$$\tilde{\theta} : G/K \cong \operatorname{im} \theta.$$

Proof

All the elements in the coset $K + g$ are mapped by θ to $(g)\theta$ because $(k + g)\theta = (k)\theta + (g)\theta = 0' + (g)\theta = (g)\theta$ for all $k \in K$. So the above definition of $\tilde{\theta}$ makes sense and produces the mapping $\tilde{\theta} : G/K \rightarrow \operatorname{im} \theta$. Suppose $(g_1)\theta = (g_2)\theta$ for $g_1, g_2 \in G$. Then $(g_1 - g_2)\theta = (g_1)\theta - (g_2)\theta = 0'$ showing that $g_1 - g_2 = k \in K$, that is, $g_1 = k + g_2$ and so g_1 and g_2 belong to the same coset of $\ker \theta$ in G . Therefore θ has a different effect on the elements of different cosets, in other words, $\tilde{\theta}$ is injective. As θ is additive, so also is $\tilde{\theta}$ because

$$\begin{aligned} ((K + g_1) + (K + g_2))\tilde{\theta} &= (K + (g_1 + g_2))\tilde{\theta} = (g_1 + g_2)\theta = (g_1)\theta + (g_2)\theta \\ &= (K + g_1)\tilde{\theta} + (K + g_2)\tilde{\theta} \quad \text{for all } g_1, g_2 \in G. \end{aligned}$$

Finally $\operatorname{im} \tilde{\theta} = \operatorname{im} \theta$ and so $\tilde{\theta}$ is surjective. Therefore $\tilde{\theta}$ is an isomorphism being bijective and additive. \square

The isomorphism $\tilde{\theta}$ is said to be *induced* by the homomorphism θ . So every homomorphism $\theta : G \rightarrow G'$ induces (gives rise to) an isomorphism $\tilde{\theta}$ as in Theorem 2.16 between the quotient group $G/\ker \theta$ and the subgroup $\operatorname{im} \theta$ of G' .

We've met particular cases of Theorem 2.16 already in our discussion of cyclic groups. Let's briefly recapitulate Theorem 2.5. Suppose that G is a cyclic group with generator g and let $\theta : \mathbb{Z} \rightarrow G$ be the \mathbb{Z} -linear mapping defined by $(m)\theta = mg$ for all $m \in \mathbb{Z}$. Then $G = \langle g \rangle = \text{im } \theta$ and $K = \ker \theta = \langle n \rangle$ is the order ideal of g where the non-negative integer n is unique. Applying Theorem 2.16 we obtain the isomorphism $\tilde{\theta} : \mathbb{Z}/\langle n \rangle \cong G$ where $(\overline{m})\tilde{\theta} = (K + m)\tilde{\theta} = (m)\theta = mg$ for all $\overline{m} \in \mathbb{Z}/\langle n \rangle$. Finally C_n is the isomorphism type of G . So the isomorphism types C_n of cyclic groups G correspond bijectively to the non-negative integers n . From the classification point of view this is all there is to know about cyclic groups!

Applying Theorem 2.16 to the natural homomorphism $\eta : \mathbb{Z} \rightarrow \mathbb{Z}_n$ produces the isomorphism $\tilde{\eta} : \mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n$ given by $(\overline{m})\tilde{\eta} = \overline{m}$ for all $m \in \mathbb{Z}$ as $\ker \eta = \langle n \rangle$. So in fact $\mathbb{Z}/\langle n \rangle = \mathbb{Z}_n$ and $\tilde{\eta}$ is the identity mapping. More generally let K be a submodule of the \mathbb{Z} -module G . Remember that the natural homomorphism $\eta : G \rightarrow G/K$ is defined by $(g)\eta = \overline{g} = K + g$ for all $g \in G$. Also remember that the 0-element of G/K is the coset $K + 0 = K$. Therefore

$$\ker \eta = \{g \in G : (g)\eta = K\} = \{g \in G : K + g = K\} = \{g \in G : g \in K\} = K.$$

We've shown that the natural homomorphism $\eta : G \rightarrow G/K$ has K as its kernel. A typical element of G/K is $K + g = (g)\eta$ and so η is surjective, that is, $\text{im } \eta = G/K$. We're ready to apply Theorem 2.16 to η and the outcome is something of an anticlimax because $\tilde{\eta} : G/K \cong G/K$ is nothing more than the identity mapping as $(\overline{g})\tilde{\eta} = \overline{g}$ for all $g \in G$.

The mapping $\theta : \mathbb{Z} \oplus \mathbb{Z} \rightarrow \mathbb{Z}$, defined by $(l, m)\theta = l - m$ for all $l, m \in \mathbb{Z}$, is additive and surjective. In this case $\text{im } \theta = \mathbb{Z}$ and $\ker \theta = \{(l, m) : (l, m)\theta = l - m = 0\} = \{(l, l) : l \in \mathbb{Z}\} = \langle (1, 1) \rangle$. From Theorem 2.16 we conclude that $(\mathbb{Z} \oplus \mathbb{Z})/\langle (1, 1) \rangle$ is an infinite cyclic group as $\tilde{\theta} : (\mathbb{Z} \oplus \mathbb{Z})/\langle (1, 1) \rangle \cong \mathbb{Z}$. Each coset of $\langle (1, 1) \rangle$ in $\mathbb{Z} \oplus \mathbb{Z}$ can be expressed as $\overline{(l, 0)}$ for a unique integer l and $(\overline{(l, 0)})\tilde{\theta} = l - 0 = l$.

Isomorphisms occur between abelian groups in additive notation and abelian groups in multiplicative notation. Let \mathbb{C}^* denote the multiplicative group of non-zero complex numbers and let $\theta : \mathbb{R} \rightarrow \mathbb{C}^*$ be the mapping defined by $(x)\theta = \cos 2\pi x + i \sin 2\pi x$ for all $x \in \mathbb{R}$. Therefore $(x)\theta$ is the complex number of modulus 1 and argument $2\pi x$. The reader will certainly know that multiplication of complex numbers is carried out by multiplying moduli and adding arguments and so

$$(x + x')\theta = (x)\theta \cdot (x')\theta \quad \text{for all } x, x' \in \mathbb{R}.$$

Therefore θ is a homomorphism from the additive group \mathbb{R} to the multiplicative group \mathbb{C}^* . In this context $\ker \theta$ consists of the real numbers x which θ maps to the identity element 1 of \mathbb{C}^* . Now $(x)\theta = 1$ if and only if x is a whole number, that is, $\ker \theta = \mathbb{Z}$. From Theorem 2.16 we deduce that $\tilde{\theta} : \mathbb{R}/\mathbb{Z} \cong \text{im } \theta$, and so \mathbb{R}/\mathbb{Z} (the reals modulo 1) is isomorphic to the group $\text{im } \theta$ of complex numbers of modulus 1.

Let G be an abelian group. Any group isomorphic to a quotient group G/K , where K is a subgroup of G , is called a *homomorphic image* of G . The reason for this terminology is as follows. Let $\theta : G \rightarrow G'$ be a homomorphism from G to an abelian group G' . Then $(G)\theta = \text{im } \theta \cong G/K$ where $K = \ker \theta$ by Theorem 2.16. So every homomorphic image $(G)\theta$ of G is isomorphic to a quotient group G/K . On the other hand, every quotient group G/K is a homomorphic image of G since $G/K = (G)\eta = \text{im } \eta$ where $\eta : G \rightarrow G/K$ is the natural homomorphism. The preceding paragraph shows that the multiplicative group of complex numbers of modulus 1 is a homomorphic image of the additive group of real numbers.

We next generalise the discussion following Lemma 2.2 by showing that every \mathbb{Z} -linear mapping gives rise to a bijective correspondence between two sets of submodules.

Theorem 2.17

Let G and G' be \mathbb{Z} -modules and let $\theta : G \rightarrow G'$ be a \mathbb{Z} -linear mapping. Let \mathbb{L} be the set of submodules H of G with $\ker \theta \subseteq H$. Let \mathbb{L}' be the set of submodules H' of G' with $H' \subseteq \text{im } \theta$. Then $(H)\theta = \{(h)\theta : h \in H\}$ is in \mathbb{L}' for all H in \mathbb{L} . The mapping $H \rightarrow (H)\theta$ is a bijection from \mathbb{L} to \mathbb{L}' and satisfies

$$H_1 \subseteq H_2 \Leftrightarrow (H_1)\theta \subseteq (H_2)\theta \quad \text{for all } H_1, H_2 \in \mathbb{L}.$$

Proof

For each submodule H of G it is routine to verify that $(H)\theta$ is a submodule of $\text{im } \theta$, and so $(H)\theta$ belongs to \mathbb{L}' for H in \mathbb{L} . For each submodule H' of $\text{im } \theta$ let $(H')\varphi = \{h \in G : (h)\theta \in H'\}$. Again it is routine to verify that $(H')\varphi$ is a submodule of G . As the zero $0'$ of G' belongs to H' we see that $\ker \theta \subseteq (H')\varphi$, that is, $(H')\varphi$ belongs to \mathbb{L} for all H' in \mathbb{L}' . The proof is completed by showing that the mapping $\mathbb{L} \rightarrow \mathbb{L}'$ given by $H \rightarrow (H)\theta$ for all $H \in \mathbb{L}$ and the mapping $\mathbb{L}' \rightarrow \mathbb{L}$ given by $H' \rightarrow (H')\varphi$ for all $H' \in \mathbb{L}'$ are inverses of each other. (The reader is reminded that only bijective mappings have inverses and often the best way (as here) of showing that a mapping is a bijection amounts to ‘conjuring up’ another mapping which turns out to be its inverse.) Notice $H \subseteq (H)\theta\varphi$ as $(h)\theta \in (H)\theta$ for all $h \in H$. Now consider $g \in (H)\theta\varphi = ((H)\theta)\varphi$. Then $(g)\theta \in (H)\theta$. So $(g)\theta = (h)\theta$ for some $h \in H$. However $g - h = k \in \ker \theta$ since $(g - h)\theta = (g)\theta - (h)\theta = 0'$. So $g = h + k \in H$ since $\ker \theta \subseteq H$ and H is closed under addition. So $(H)\theta\varphi \subseteq H$. Therefore $H = (H)\theta\varphi$ for all H in \mathbb{L} .

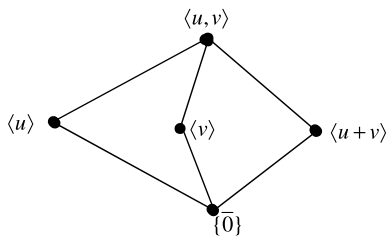
In a similar way $(H')\varphi\theta = ((H')\varphi)\theta \subseteq H'$ since $(g)\theta \in H'$ for all $g \in (H')\varphi$. Let $h' \in H'$. Then $h' = (g)\theta$ for $g \in G$ since $H' \subseteq \text{im } \theta$. But $(g)\theta \in H'$ means $g \in (H')\varphi$ and so $h' = (g)\theta \in ((H')\varphi)\theta = (H')\varphi\theta$. We’ve shown $H' \subseteq (H')\varphi\theta$ and so $H' =$

$(H')\varphi\theta$ for all H' in \mathbb{L}' . The mapping $\mathbb{L} \rightarrow \mathbb{L}'$, in which $H \rightarrow (H)\theta$, has an inverse and so this mapping is bijective. Finally it's straightforward to show that $H_1 \subseteq H_2 \Rightarrow (H_1)\theta \subseteq (H_2)\theta$ for $H_1, H_2 \in \mathbb{L}$. Now suppose $(H_1)\theta \subseteq (H_2)\theta$ for $H_1, H_2 \in \mathbb{L}$. Then $H_1 = (H_1)\theta\varphi \subseteq (H_2)\theta\varphi = H_2$ and therefore

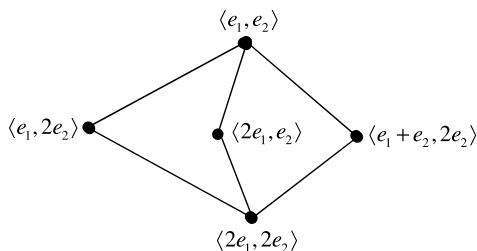
$$H_1 \subseteq H_2 \quad \Leftrightarrow \quad (H_1)\theta \subseteq (H_2)\theta. \quad \square$$

Each pair of submodules H_1 and H_2 in \mathbb{L} gives rise to submodules $H_1 \cap H_2$ and $H_1 + H_2$ in \mathbb{L} . The set \mathbb{L} , partially ordered by inclusion, is therefore a *lattice* as is \mathbb{L}' . We shall not have much to say about lattices *per se*, but it is often illuminating to draw their diagrams as below.

We return to the \mathbb{Z} -linear mapping $\theta : \mathbb{Z} \oplus \mathbb{Z} \rightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$ mentioned before Theorem 2.11. So $(l, m)\theta = lu + mv = (\bar{l}, \bar{m}) \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$ for all $l, m \in \mathbb{Z}$, where $u = (\bar{1}, \bar{0})$, $v = (\bar{0}, \bar{1}) \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$. The Klein 4-group $\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \langle u, v \rangle = \text{im } \theta$ has five subgroups $\{\bar{0}\}, \langle u \rangle, \langle v \rangle, \langle u + v \rangle, \langle u, v \rangle$. These are the subgroups H' of Theorem 2.17 shown in their lattice diagram:



The five corresponding subgroups $H = (H')\varphi = \{(l, m) \in \mathbb{Z} \oplus \mathbb{Z} : (\bar{l}, \bar{m}) \in H'\}$ of $\mathbb{Z} \oplus \mathbb{Z}$ are $\langle 2e_1, 2e_2 \rangle$, $\langle e_1, 2e_2 \rangle$, $\langle 2e_1, e_2 \rangle$, $\langle e_1 + e_2, 2e_2 \rangle$, $\langle e_1, e_2 \rangle$ respectively and by Theorem 2.17 they fit together in the same way:



Notice that $\langle e_1 + e_2, 2e_2 \rangle = \langle e_1 + e_2, 2e_1 \rangle = \{(l, m) : \text{parity } l = \text{parity } m\}$. Each of these subgroups H has a \mathbb{Z} -basis as shown, that is, each element of H is uniquely ex-

pressible as an integer linear combination of the \mathbb{Z} -basis elements which themselves belong to H . We show in Theorem 3.1 that *all* subgroups H of $\mathbb{Z} \oplus \mathbb{Z}$ have \mathbb{Z} -bases. This fact allows the abstract theory to be expressed using matrices over \mathbb{Z} : for each subgroup H we construct a matrix A over \mathbb{Z} having as its rows a set of generators of H . So the above five subgroups H of $\mathbb{Z} \oplus \mathbb{Z}$ give rise to the following five 2×2 matrices A over \mathbb{Z} :

$$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

We develop this idea in Chapter 3. For the moment notice that the invariant factors of these matrices present the isomorphism types of the corresponding quotient groups $\mathbb{Z} \oplus \mathbb{Z}/H \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2/H'$ on a plate! Thus $\mathbb{Z} \oplus \mathbb{Z}/\langle 2e_1, 2e_2 \rangle \cong \mathbb{Z}/\langle 2 \rangle \oplus \mathbb{Z}/\langle 2 \rangle$ has isomorphism type $C_2 \oplus C_2$ being the direct sum of two cyclic groups of type C_2 . Similarly $\mathbb{Z} \oplus \mathbb{Z}/\langle e_1, 2e_2 \rangle \cong \mathbb{Z}/\langle 1 \rangle \oplus \mathbb{Z}/\langle 2 \rangle$ has isomorphism type $C_1 \oplus C_2 = C_2$ as the trivial C_1 term can be omitted. The second, third and fourth of the above matrices are equivalent over \mathbb{Z} , the corresponding quotient groups being isomorphic. Also $\mathbb{Z} \oplus \mathbb{Z}/\langle e_1, e_2 \rangle \cong \mathbb{Z}/\langle 1 \rangle \oplus \mathbb{Z}/\langle 1 \rangle$ has isomorphism type $C_1 \oplus C_1 = C_1$.

Much of the abstract theory of subgroups and quotient groups developed here applies, with some minor changes, to non-abelian groups G , which are usually expressed in multiplicative notation. For such groups the quotient group G/K makes sense only when K is a *normal subgroup* of G , that is,

$$Kg = gK \quad \text{for all } g \text{ in } G.$$

The above equation means each element kg for $k \in K$, $g \in G$ can be expressed as gk' for some $k' \in K$, and conversely each element gk' for $g \in G$, $k' \in K$ can be expressed as kg for some $k \in K$. The kernel of every homomorphism $\theta : G \rightarrow G'$ between groups is a normal subgroup of G . Lagrange's theorem and the conclusions of Theorems 2.16 and 2.17 are valid for groups in general (see Exercises 2.3, Question 4).

We now discuss (finitely generated) free \mathbb{Z} -modules. In fact the following theory 'works' when \mathbb{Z} is replaced by any non-trivial commutative ring R with 1-element. The theory of determinants extends to square matrices over R as was pointed out in Section 1.3. So a $t \times t$ matrix P over R is invertible over R if and only if $\det P \in U(R)$, that is, the determinant of P is an invertible element of R .

Lemma 2.18

Let P and Q be $t \times t$ matrices over a non-trivial commutative ring R such that $PQ = I$ where I is the $t \times t$ identity matrix over R . Then $QP = I$.

Proof

Comparing determinants in the matrix equation $PQ = I$ gives $\det PQ = \det I = 1$ the 1-element of R . Using the multiplicative property Theorem 1.18 of determinants we obtain $(\det P)(\det Q) = 1$ and so $\det P$ is an invertible element of R . The matrix $P^{-1} = (1/\det P) \operatorname{adj} P$ over R satisfies $P^{-1}P = I = PP^{-1}$. Hence $P^{-1} = P^{-1}I = P^{-1}PQ = IQ = Q$ and so $QP = P^{-1}P = I$. \square

Interchanging the roles of P and Q we see that $QP = I \Rightarrow PQ = I$. So from the single equation $PQ = I$ we can deduce that P and Q are both invertible over R and each is the inverse of the other: $Q = P^{-1}$ and $P = Q^{-1}$. We will need this fact in the proof of the next theorem.

The set of $t \times t$ matrices over the ring R is closed under matrix addition and matrix multiplication and is itself a ring $\mathfrak{M}_t(R)$. The invertible elements of $\mathfrak{M}_t(R)$ form the *general linear group* $GL_t(R)$ of degree t over R . We will study certain aspects of $\mathfrak{M}_t(F)$, where F is a field, in the second half of the book. Let us suppose that F is a *finite* field with q elements. You should be aware that q must be a power of a prime (Exercises 2.3, Question 5(a)). Then $|\mathfrak{M}_t(F)| = q^{t^2}$, there being q choices for each of the t^2 entries in a $t \times t$ matrix over F . How can we find the number $|GL_t(F)|$ of invertible $t \times t$ matrices P over F ? The reader will know that P is invertible over F if and only if the rows of P form a basis of the vector space F^t of all t -tuples over F . What is more each basis v_1, v_2, \dots, v_t of F^t can be built up, vector by vector, ensuring linear independence at each stage as we now explain. There are $q^t - 1$ choices for v_1 (any of the $|F^t| = q^t$ vectors in F^t except the zero vector). Suppose i linearly independent vectors v_1, v_2, \dots, v_i have been chosen where $1 \leq i < t$. Then $v_1, v_2, \dots, v_i, v_{i+1}$ are linearly independent $\Leftrightarrow v_{i+1} \notin \langle v_1, v_2, \dots, v_i \rangle$. So there are $q^t - q^i$ choices for v_{i+1} (any of the $|F^t| = q^t$ vectors in F^t except for the $q^i = |\langle v_1, v_2, \dots, v_i \rangle|$ vectors in $\langle v_1, v_2, \dots, v_i \rangle$). Hence

$$|GL_t(F)| = (q^t - 1)(q^t - q)(q^t - q^2) \cdots (q^t - q^{t-1})$$

there being $q^t - q^i$ remaining choices for row $i + 1$ of a matrix P in $GL_t(F)$, the previous i rows of P having already been chosen. In particular the number of 3×3 matrices over \mathbb{Z}_2 is $2^9 = 512$ and $(2^3 - 1)(2^3 - 2)(2^3 - 4) = 7 \times 6 \times 4 = 168$ of these are invertible. So $|\mathfrak{M}_3(\mathbb{Z}_2)| = 512$ and $|GL_3(\mathbb{Z}_2)| = 168$.

The Chinese remainder theorem generalises to decompose $\mathfrak{M}_t(\mathbb{Z}_{mn})$ where $\gcd\{m, n\} = 1$ using the ring isomorphism $\alpha : \mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$ of Theorem 2.11 as follows: let \bar{r}_{mn} denote the (i, j) -entry in the $t \times t$ matrix A over \mathbb{Z}_{mn} for $1 \leq i, j \leq t$. Write $(A)\alpha = (B, C)$ where B is the $t \times t$ matrix over \mathbb{Z}_m with (i, j) -entry \bar{r}_m and C is the $t \times t$ matrix over \mathbb{Z}_n with (i, j) -entry \bar{r}_n , that is, B and C are obtained by reducing each entry in A modulo m and modulo n respectively. Then

$$\alpha : \mathfrak{M}_t(\mathbb{Z}_{mn}) \cong \mathfrak{M}_t(\mathbb{Z}_m) \oplus \mathfrak{M}_t(\mathbb{Z}_n) \quad \text{for } \gcd\{m, n\} = 1$$

as α is a ring isomorphism. So α maps invertible elements to invertible elements and hence we obtain the group isomorphism

$$\alpha| : GL_t(\mathbb{Z}_{mn}) \cong GL_t(\mathbb{Z}_m) \times GL_t(\mathbb{Z}_n) \quad \text{for } \gcd\{m, n\} = 1$$

where the right-hand side denotes the *external direct product* of the indicated groups (see Exercises 2.3, Question 4(d)) and $\alpha|$ denotes the restriction of α to $GL_t(\mathbb{Z}_{mn})$.

For example take $t = 2$, $m = 7$, $n = 8$ and

$$A = \begin{pmatrix} \overline{27} & \overline{17} \\ \overline{44} & \overline{51} \end{pmatrix} \in \mathfrak{M}_2(\mathbb{Z}_{56}).$$

Then

$$(A)\alpha = (B, C) = \left(\begin{pmatrix} \overline{6} & \overline{3} \\ \overline{2} & \overline{2} \end{pmatrix}, \begin{pmatrix} \overline{3} & \overline{1} \\ \overline{4} & \overline{3} \end{pmatrix} \right) \in \mathfrak{M}_2(\mathbb{Z}_7) \oplus \mathfrak{M}_2(\mathbb{Z}_8).$$

In fact A , B and C are invertible and

$$(A^{-1})\alpha = (B^{-1}, C^{-1}) = \left(\begin{pmatrix} \overline{5} & \overline{3} \\ \overline{2} & \overline{1} \end{pmatrix}, \begin{pmatrix} \overline{7} & \overline{3} \\ \overline{4} & \overline{7} \end{pmatrix} \right).$$

Hence

$$A^{-1} = \begin{pmatrix} \overline{47} & \overline{3} \\ \overline{44} & \overline{15} \end{pmatrix}$$

on applying Theorem 2.11 to each entry. Note $|\mathfrak{M}_2(\mathbb{Z}_{56})| = 56^4$ and

$$|GL_2(\mathbb{Z}_{56})| = |GL_2(\mathbb{Z}_7)| \times |GL_2(\mathbb{Z}_8)| = (7^2 - 1)(7^2 - 7) \times 4^4 \times 6 = 3096576$$

as

$$|GL_2(\mathbb{Z}_8)| = 4^4 \times |GL_2(\mathbb{Z}_2)|.$$

More generally let $\det A = \overline{m}$ where $A \in \mathfrak{M}_t(\mathbb{Z}_n)$. As \overline{m} is an invertible element of $\mathbb{Z}_n \Leftrightarrow \gcd\{m, n\} = 1$, we see that $A \in GL_t(\mathbb{Z}_n) \Leftrightarrow \gcd\{m, n\} = 1$. Also $|GL_t(\mathbb{Z}_q)| = p^{t^2(s-1)}|GL_t(\mathbb{Z}_p)|$ where $q = p^s$, p prime (see Exercises 2.3, Question 5(b)).

In Chapter 5 we use the concept of an $F[x]$ -module M in order to discuss the theory of *similarity* of square matrices over the field F . Here $F[x]$ is the ring of all polynomials $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ over F . There is a close analogy between the theory of similarity and the theory of finite abelian groups as we'll come to realise. Both theories involve R -modules where R is a principal ideal domain. However, the aspect of the theory which we deal with next 'works' in the general context of R being merely a non-trivial commutative ring (with 1-element). So we assume in the following theory that R is such a ring.

Let M be a set closed under a binary operation called ‘addition’ and denoted in the familiar way by ‘+’. Suppose that $(M, +)$ satisfies laws 1, 2, 3 and 4 of an abelian group as introduced at the beginning of Section 2.1. Suppose also that it makes sense to multiply elements r of a commutative ring R and elements v of M together, the result always being an element of M , that is,

$$rv \in M \quad \text{for all } r \in R, v \in M.$$

Then M is called an R -module if the above product rv satisfies:

5. $r(v_1 + v_2) = rv_1 + rv_2$ for all $r \in R$ and all $v_1, v_2 \in M$,
 $(r_1 + r_2)v = r_1v + r_2v$ for all $r_1, r_2 \in R$ and all $v \in M$,
6. $(r_1r_2)v = r_1(r_2v)$ for all $r_1, r_2 \in R$ and all $v \in M$,
7. $1v = v$ for all $v \in M$ where 1 denotes the 1-element of R .

There are no surprises here! We have simply mimicked the \mathbb{Z} -module definition at the start of Section 2.1. Should the ring R happen to be a field F then laws 1–7 above are the laws of a vector space, that is,

the concepts F -module and vector space over F are the same.

Definition 2.19

Let M be an R -module containing v_1, v_2, \dots, v_t .

- (i) The elements v_1, v_2, \dots, v_t generate M if each element of M can be expressed $r_1v_1 + r_2v_2 + \dots + r_tv_t$ for some $r_1, r_2, \dots, r_t \in R$ in which case we write

$$M = \langle v_1, v_2, \dots, v_t \rangle.$$

- (ii) The elements v_1, v_2, \dots, v_t are R -independent if the equation

$$r_1v_1 + r_2v_2 + \dots + r_tv_t = 0$$

holds only in the case $r_1 = r_2 = \dots = r_t = 0$.

- (iii) The ordered set v_1, v_2, \dots, v_t is an R -basis of M if v_1, v_2, \dots, v_t generate M and are R -independent.

The above definitions are modelled on the corresponding vector space concepts which will be well-known to the reader. You are used to regarding the bases v_1, v_2 and v_2, v_1 of a 2-dimensional vector space V as being different – the order in which the vectors appear is important and the same goes for R -bases.

Let the R -module M have R -basis v_1, v_2, \dots, v_t and let $v \in M$. As v_1, v_2, \dots, v_t generate M there are ring elements r_1, r_2, \dots, r_t with $v = r_1v_1 + r_2v_2 + \dots + r_tv_t$.

In fact r_1, r_2, \dots, r_t are unique because suppose $v = r'_1 v_1 + r'_2 v_2 + \dots + r'_t v_t$ where $r'_1, r'_2, \dots, r'_t \in R$. Subtracting we obtain

$$0 = v - v = (r_1 - r'_1)v_1 + (r_2 - r'_2)v_2 + \dots + (r_t - r'_t)v_t$$

and so from the R -independence of v_1, v_2, \dots, v_t we deduce $r_1 - r'_1 = 0, r_2 - r'_2 = 0, \dots, r_t - r'_t = 0$; therefore $r_i = r'_i$ for $1 \leq i \leq t$, showing that each v in M can be expressed in one and only one way as an R -linear combination of v_1, v_2, \dots, v_t . In particular (as in the next proof) from $v_i = r_1 v_1 + r_2 v_2 + \dots + r_t v_t$ we deduce $r_i = 1$ and $r_k = 0$ for $k \neq i$.

It is not encouraging that some generating sets of a \mathbb{Z} -module G do not contain any \mathbb{Z} -basis of G , that some \mathbb{Z} -independent subsets of G are not contained in any \mathbb{Z} -basis of G , and that quite possibly G has no \mathbb{Z} -basis at all. However, as a consequence of the next theorem, should an R -module M have an R -basis consisting of exactly t (a non-negative integer) elements then every R -basis of M has t elements also, in which case M is said to be a *free R -module of rank t* .

Theorem 2.20

Let R be a non-trivial commutative ring and suppose that M is an R -module with R -basis v_1, v_2, \dots, v_t . Suppose also that M contains elements u_1, u_2, \dots, u_s which generate M . Then $s \geq t$.

Proof

Each v_i is a linear combination of u_1, u_2, \dots, u_s and so there are ring elements $p_{ij} \in R$ with $v_i = \sum_{j=1}^s p_{ij} u_j$ for $1 \leq i \leq t$. Let $P = (p_{ij})$ denote the $t \times s$ matrix over R with (i, j) -entry p_{ij} . In the same way each module element u_j is expressible as a linear combination of v_1, v_2, \dots, v_t and so there are ring elements $q_{jk} \in R$ with $u_j = \sum_{k=1}^t q_{jk} v_k$ for $1 \leq j \leq s$. Let $Q = (q_{jk})$ be the $s \times t$ matrix over R with (j, k) -entry q_{jk} . We've chosen the symbols i, j, k so that the (i, k) -entry $\sum_{j=1}^s p_{ij} q_{jk}$ in the $t \times t$ matrix PQ appears in the familiar notation. Substituting for u_j we obtain

$$v_i = \sum_{j=1}^s p_{ij} u_j = \sum_{j=1}^s p_{ij} \left(\sum_{k=1}^t q_{jk} v_k \right) = \sum_{k=1}^t \left(\sum_{j=1}^s p_{ij} q_{jk} \right) v_k \quad \text{for } 1 \leq i \leq t$$

which must in fact be no more than the unsurprising equation $v_i = v_i$ as v_1, v_2, \dots, v_t are R -independent. Looking at the last term above we see that the (i, k) -entry in PQ is 1 or 0 according as $i = k$ or $i \neq k$, that is,

$$PQ = I_t \quad \text{the } t \times t \text{ identity matrix over } R. \quad (\diamond)$$

Suppose $s < t$. We'll shortly discover a contradiction to this supposition and that will complete the proof. We can't use Lemma 2.18 and leap to the conclusion that P and Q are inverses of each other as neither P nor Q is a square matrix. But the reader should have the feeling that something is wrong: the condition $s < t$ means that P is 'long and thin' and Q is 'short and fat', but nevertheless their product PQ is the large 'virile' identity matrix I_t . We clinch the matter by partitioning $P = \begin{pmatrix} P_1 \\ P_2 \end{pmatrix}$ and $Q = (Q_1 \mid Q_2)$ where P_1 and Q_1 are $s \times s$ matrices, and so P_2 is $(t-s) \times s$ and Q_2 is $s \times (t-s)$. Then \spadesuit gives

$$PQ = \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} (Q_1 \mid Q_2) = \left(\begin{array}{c|c} P_1 Q_1 & P_1 Q_2 \\ \hline P_2 Q_1 & P_2 Q_2 \end{array} \right) = I_t = \left(\begin{array}{c|c} I_s & 0 \\ \hline 0 & I_{t-s} \end{array} \right)$$

and so $P_1 Q_1 = I_s$ on comparing leading entries. Now Lemma 2.18 can be used to give $Q_1 P_1 = I_s$ as the $s \times s$ matrices P_1 and Q_1 are inverses of each other. Comparing $(1, 2)$ -entries in the above partitioned matrices gives $P_1 Q_2 = 0$ and hence $Q_2 = I_s Q_2 = (Q_1 P_1) Q_2 = Q_1 (P_1 Q_2) = Q_1 0 = 0$. The 1-element of R cannot be zero (for if so then $R = \{0\}$). Comparing $(2, 2)$ -entries above now gives $P_2 Q_2 = I_{t-s} \neq 0$ whereas $P_2 Q_2 = P_2 0 = 0$. We have found the contradiction to $s < t$ we are looking for as $P_2 Q_2$ cannot be both non-zero and zero! Therefore $s \geq t$. \square

Corollary 2.21

Let M be an R -module with R -basis v_1, v_2, \dots, v_t . Then every R -basis of M has exactly t elements. Let u_1, u_2, \dots, u_t be elements of M and let $Q = (q_{jk})$ be the $t \times t$ matrix over R such that $u_j = \sum_{k=1}^t q_{jk} v_k$ for $1 \leq j \leq t$. Then u_1, u_2, \dots, u_t is an R -basis of M if and only if Q is invertible over R .

Proof

Let u_1, u_2, \dots, u_s be an R -basis of M . As u_1, u_2, \dots, u_s generate M we deduce $t \leq s$ from Theorem 2.20. As u_1, u_2, \dots, u_s is an R -basis of M and v_1, v_2, \dots, v_t generate M , interchanging the roles of the u 's and v 's, we obtain $s \leq t$ from Theorem 2.20. So $s = t$. Using \spadesuit above and Lemma 2.18 we see that the $t \times t$ matrix Q is invertible over R .

Now suppose that u_1, u_2, \dots, u_t are elements of M such that Q is invertible over R . Write $Q^{-1} = (p_{ij})$. Multiplying $u_j = \sum_{k=1}^t q_{jk} v_k$ by p_{ij} and summing over j gives

$$\sum_{j=1}^t p_{ij} u_j = \sum_{j=1}^t p_{ij} \left(\sum_{k=1}^t q_{jk} v_k \right) = \sum_{k=1}^t \left(\sum_{j=1}^t p_{ij} q_{jk} \right) v_k = v_i \quad \text{for } 1 \leq i \leq t \quad (\heartsuit)$$

which shows that each v_i is an R -linear combination of u_1, u_2, \dots, u_t . Consider $v \in M$. As $M = \langle v_1, v_2, \dots, v_t \rangle$ there are elements $r_1, r_2, \dots, r_t \in R$ with $v = \sum_{i=1}^t r_i v_i$. Using (♥) we see

$$v = \sum_{i=1}^t r_i \left(\sum_{j=1}^t p_{ij} u_j \right) = \sum_{j=1}^t \left(\sum_{i=1}^t r_i p_{ij} \right) u_j = \sum_{j=1}^t r'_j u_j$$

where $r'_j = \sum_{i=1}^t r_i p_{ij}$ for $1 \leq j \leq t$, that is, $(r'_1, r'_2, \dots, r'_t) = (r_1, r_2, \dots, r_t) Q^{-1}$. So u_1, u_2, \dots, u_t generate M .

Finally we show that u_1, u_2, \dots, u_t are R -independent. Suppose $\sum_{j=1}^t r'_j u_j = 0$ where $r'_1, r'_2, \dots, r'_t \in R$. On multiplying $u_j = \sum_{k=1}^t q_{jk} v_k$ by r'_j and summing over j we obtain

$$0 = \sum_{j=1}^t r'_j u_j = \sum_{j=1}^t r'_j \left(\sum_{k=1}^t q_{jk} v_k \right) = \sum_{k=1}^t \left(\sum_{j=1}^t r'_j q_{jk} \right) v_k = \sum_{k=1}^t r_k v_k$$

where $r_k = \sum_{j=1}^t r'_j q_{jk}$ for $1 \leq k \leq t$, that is, $(r_1, r_2, \dots, r_t) = (r'_1, r'_2, \dots, r'_t) Q$. As v_1, v_2, \dots, v_t are R -independent we see $r_1 = r_2 = \dots = r_t = 0$. Hence $(r'_1, r'_2, \dots, r'_t) = (r_1, r_2, \dots, r_t) Q^{-1} = 0 \times Q^{-1} = 0$ showing $r'_1 = r'_2 = \dots = r'_t = 0$. So u_1, u_2, \dots, u_t are R -independent and hence they form an R -basis of M . \square

Definition 2.22

Let R be a commutative ring. An R -module M having an R -basis is called *free*. The number t of elements in any R -basis of a free R -module M is called the *rank* of M .

So the concept ‘rank of a module’ applies only to free modules. This concept makes sense for R -modules by Corollary 2.21 and generalises the familiar idea of dimension of a finite-dimensional vector space. We’ll use rank as defined in Definition 2.22 to establish the important *Invariance Theorem* 3.7 concerning f.g. \mathbb{Z} -modules in Section 3.1.

The set R^t of t -tuples (r_1, r_2, \dots, r_t) , where each r_i belongs to the non-trivial commutative ring R , is itself an R -module, the module operations being carried out componentwise. It should come as no surprise to the reader that R^t has an R -basis, namely

$$e_1 = (1, 0, 0, \dots, 0), \quad e_2 = (0, 1, 0, \dots, 0), \quad \dots, \quad e_t = (0, 0, 0, \dots, 1)$$

which is known as the *standard basis* of R^t . So R^t is free of rank t .

Our next corollary tells us how to recognise R -bases of R^t : they are nothing more than the rows of invertible $t \times t$ matrices over R .

Corollary 2.23

Let $\rho_1, \rho_2, \dots, \rho_t$ denote the rows of the $t \times t$ matrix Q over a non-trivial commutative ring R . Then $\rho_1, \rho_2, \dots, \rho_t$ is an R -basis of R^t if and only if Q is invertible over R .

Proof

Write $Q = (q_{jk})$. Then $\rho_j = \sum_{k=1}^t q_{jk} e_k$ for $1 \leq j \leq t$. On applying Corollary 2.21 with $M = R^t$, $u_j = \rho_j$ and $v_k = e_k$ we see that $\rho_1, \rho_2, \dots, \rho_t$ is an R -basis of R^t if and only if Q is invertible over R . \square

We'll use the case $R = \mathbb{Z}$ of Corollary 2.23 in Section 3.1. As an illustration consider $\rho_1 = (4, 5)$, $\rho_2 = (5, 6)$. Then ρ_1, ρ_2 is a \mathbb{Z} -basis of \mathbb{Z}^2 as $P = \begin{pmatrix} \rho_1 \\ \rho_2 \end{pmatrix} = \begin{pmatrix} 4 & 5 \\ 5 & 6 \end{pmatrix}$ is invertible over \mathbb{Z} since $\det P = -1$ is an invertible element of \mathbb{Z} . The rows of $P^{-1} = \begin{pmatrix} -6 & 5 \\ 5 & -4 \end{pmatrix}$ tell us how the elements e_1, e_2 of the standard \mathbb{Z} -basis of \mathbb{Z}^2 are expressible as \mathbb{Z} -linear combinations of ρ_1, ρ_2 because

$$\begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = I = P^{-1}P = \begin{pmatrix} -6 & 5 \\ 5 & -4 \end{pmatrix} \begin{pmatrix} \rho_1 \\ \rho_2 \end{pmatrix} = \begin{pmatrix} -6\rho_1 + 5\rho_2 \\ 5\rho_1 - 4\rho_2 \end{pmatrix},$$

that is, $e_1 = -6\rho_1 + 5\rho_2$, $e_2 = 5\rho_1 - 4\rho_2$ on equating rows. Hence $(m_1, m_2) = (-6m_1 + 5m_2)\rho_1 + (5m_1 - 4m_2)\rho_2$ for all $(m_1, m_2) \in \mathbb{Z}^2$, showing explicitly that ρ_1, ρ_2 generate \mathbb{Z}^2 , that is, $\langle \rho_1, \rho_2 \rangle = \mathbb{Z}^2$.

Definition 2.24

Let M and M' be R -modules. A mapping $\theta : M \rightarrow M'$ is called *R -linear* if $(v_1 + v_2)\theta = (v_1)\theta + (v_2)\theta$ for all $v_1, v_2 \in M$ and $(rv)\theta = r((v)\theta)$ for all $r \in R$, $v \in M$. A bijective R -linear mapping θ is called an *isomorphism*. If there is an isomorphism $\theta : M \rightarrow M'$, then the R -modules M and M' are called *isomorphic* and we write $\theta : M \cong M'$.

The above definition mimics Definitions 2.3 and 2.4 replacing \mathbb{Z} by the commutative ring R . The following lemma will be used in Section 3.1.

Lemma 2.25

Let M be a free R -module of rank t and let M' be an R -module which is isomorphic to M . Then M' is also free of rank t .

Proof

There is an isomorphism $\theta : M \cong M'$. The free R -module M has an R -basis v_1, v_2, \dots, v_t . Write $v'_i = (v_i)\theta$ for $1 \leq i \leq t$. It is straightforward to show that v'_1, v'_2, \dots, v'_t is an R -basis of M' (see Exercises 2.3, Question 7(a)). Hence M' is free of rank t by Definition 2.22. \square

One advantage of expressing abelian groups in the language of \mathbb{Z} -modules is that some theorems we have already met painlessly generalise to R -modules. In particular this is true of Lemma 2.10, Theorems 2.16 and 2.17 as we now outline.

Definition 2.26

Let N be a subset of an R -module M . Suppose that N is a subgroup of the additive group of M and $ru \in N$ for all $r \in R$ and all $u \in N$. Then N is called a *submodule* of the R -module M .

So submodules of the R -module M are subgroups N of the abelian group $(M, +)$ which are closed under multiplication by elements of the ring R . It is important to realise that submodules of R -modules are themselves R -modules: laws 1–7 of an R -module hold with M replaced by N throughout. The reader will be familiar with this type of thing as subspaces of vector spaces are vector spaces ‘in their own right’. Indeed should the ring R be a field F , then Definition 2.26 tells us that submodules of the F -module M are exactly subspaces of the vector space M .

Let N be a submodule of the R -module M . As N is a subgroup of the additive group M the quotient group M/N can be constructed as in Lemma 2.10 (here M and N replace G and K respectively). The elements of M/N are cosets $N + v$ for $v \in M$ where (unsurprisingly) $N + v = \{u + v : u \in N\}$. Can the abelian group M/N be given the extra structure of an R -module? The answer is: Yes!

Lemma 2.27

Let N be a submodule of the R -module M . Write $r(N + v) = N + rv$ for $r \in R$ and $v \in M$. This product is unambiguously defined and using it M/N is an R -module. The natural mapping $\eta : M \rightarrow M/N$ is R -linear where $(v)\eta = N + v$ for all $v \in N$.

Proof

Suppose $N + v = N + v'$ where $v, v' \in M$. Then $v - v' \in N$ as in Lemma 2.9. So $rv - rv' = r(v - v') \in N$ as N is a submodule of the R -module M . But $rv - rv' \in N$

gives $N + rv = N + rv'$ by Lemma 2.9 and shows that the given definition of $r(N + v)$ is unambiguous.

By Lemma 2.10 coset addition in M/N obeys laws 1, 2, 3, 4 of a \mathbb{Z} -module. We should check that laws 5, 6 and 7 are obeyed by the product $r(N + v)$ defined above. Consider $r \in R$ and $v, v_1, v_2 \in M$. Then

$$\begin{aligned} r((N + v_1) + (N + v_2)) &= r(N + (v_1 + v_2)) = N + r(v_1 + v_2) \\ &= N + (rv_1 + rv_2) = (N + rv_1) + (N + rv_2) \\ &= r(N + v_1) + r(N + v_2) \end{aligned}$$

which shows that the first part of law 5 is obeyed. The remaining parts can be checked in a similar way (see Exercises 2.3, Question 7(d)) showing that M/N is an R -module.

As $(rv)\eta = N + rv = r(N + v) = r((v)\eta)$ for all $r \in R, v \in M$ we see that η is R -linear. \square

The reader should verify that kernels and images of R -linear mappings are submodules (see Exercises 2.3, Question 7(c)).

We are now ready to generalise Theorem 2.16 and 2.17.

Corollary 2.28 (The first isomorphism theorem for R -modules)

Let M and M' be R -modules and let $\theta : M \rightarrow M'$ be an R -linear mapping. Write $K = \ker \theta$. Then $\tilde{\theta} : M/K \cong \text{im } \theta$ is an isomorphism of R -modules where $\tilde{\theta}$ is defined by $(K + v)\tilde{\theta} = (v)\theta$ for all $v \in M$.

Proof

By Theorem 2.16 we know that $\tilde{\theta}$ is an isomorphism of \mathbb{Z} -modules. So it is enough to check that $\tilde{\theta}$ is R -linear: $(r(K + v))\tilde{\theta} = (K + rv)\tilde{\theta} = (rv)\theta = r((v)\theta) = r((K + v)\tilde{\theta})$ for $r \in R, v \in M$ using the R -linearity of θ and the definition of $\tilde{\theta}$. \square

Corollary 2.29

Let M and M' be R -modules and let $\theta : M \rightarrow M'$ be an R -linear mapping. Let \mathbb{L} be the set of submodules N of M with $\ker \theta \subseteq N$. Let \mathbb{L}' be the set of submodules N' of M' with $N' \subseteq \text{im } \theta$. Then $(N)\theta = \{(u)\theta : u \in N\}$ is in \mathbb{L}' for all N in \mathbb{L} . The mapping $N \rightarrow (N)\theta$ is a bijection from \mathbb{L} to \mathbb{L}' and satisfies $N_1 \subseteq N_2 \Leftrightarrow (N_1)\theta \subseteq (N_2)\theta$ for all $N_1, N_2 \in \mathbb{L}$.

Proof

In view of Theorem 2.17 there is not a great deal left to prove and what's left is routine. We know that $(N)\theta$ is a subgroup of $(M', +)$. Consider $r \in R$ and $u \in N$. Then $ru \in N$ as N is a submodule of M . So $r((u)\theta) = (ru)\theta \in (N)\theta$ showing that $(N)\theta$ is a submodule of M' . Therefore $N \rightarrow (N)\theta$ is a mapping from \mathbb{L} to \mathbb{L}' . Following the proof of Theorem 2.17 for each submodule N' of M' write $(N')\varphi = \{v \in M : (v)\theta \in N'\}$. The diligent reader will have checked that $(N')\varphi$ is a subgroup of $(M, +)$. Consider $r \in R$ and $v \in (N')\varphi$. Is $rv \in (N')\varphi$? Yes it is, as $v' = (v)\theta \in N'$ and so $(rv)\theta = r((v)\theta) = rv' \in N'$ as N' is a submodule of M' . The conclusion is: $(N')\varphi$ is a submodule of M and $N' \rightarrow (N')\varphi$ is a mapping from \mathbb{L}' to \mathbb{L} . As before these mappings are inverses of each other and are inclusion-preserving. Therefore $N \rightarrow (N)\theta$ is a bijection from \mathbb{L} to \mathbb{L}' satisfying $N_1 \subseteq N_2 \Leftrightarrow (N_1)\theta \subseteq (N_2)\theta$ for all $N_1, N_2 \in \mathbb{L}$. \square

EXERCISES 2.3

1. (a) Let G and G' be \mathbb{Z} -modules and let $\theta : G \rightarrow G'$ be a \mathbb{Z} -linear mapping.
 - (i) Show that $\ker \theta$ is a submodule of G . Show that $\ker \theta = \{0\} \Leftrightarrow \theta$ is injective.
 - (ii) Show that $\text{im } \theta$ is a submodule of G' . Is it true that $\text{im } \theta = G' \Leftrightarrow \theta$ is surjective?
- (b) The \mathbb{Z} -linear mapping $\theta : \mathbb{Z} \oplus \mathbb{Z} \rightarrow \mathbb{Z}$ is given by $(l, m)\theta = 4l - 2m$ for all $l, m \in \mathbb{Z}$. Verify that $(1, 2) \in \ker \theta$. Do $(-1, -2)$ and $(2, 4)$ belong to $\ker \theta$? Show that $\ker \theta = \langle (1, 2) \rangle$. Which integers belong to $\text{im } \theta$? Is $\text{im } \theta$ infinite cyclic? Using the notation of Theorem 2.16, are the integers $(\ker \theta + (12, 20))\tilde{\theta}$ and $(\ker \theta + (17, 30))\tilde{\theta}$ equal? Show that $\mathbb{Z} \oplus \mathbb{Z} / \ker \theta$ is infinite cyclic and specify a generator.
- (c) Specify the subgroups of each of the following groups and hence determine the isomorphism types of their homomorphic images.
 - (i) \mathbb{Z}_8 ; (ii) \mathbb{Z}_{12} ; (iii) \mathbb{Z}_n ($n > 0$);
 - (iv) \mathbb{Z} ; (v) $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.
- (d) Let G_1 and G_2 be additive abelian groups. By applying Theorem 2.16 to suitable homomorphisms, establish the isomorphisms: $G_1/\{0\} \cong G_1$, $G_1/G_1 \cong \{0\}$. Show also that G_1 and G_2 are homomorphic images of $G_1 \oplus G_2$. Are the groups G_1 and $(G_1 \oplus G_1)/K$ isomorphic where $K = \{(g_1, g_1) : g_1 \in G_1\}$?
- (e) Let G be a \mathbb{Z} -module and $\theta : G \rightarrow G$ a \mathbb{Z} -linear mapping which is idempotent (i.e. $\theta^2 = \theta$). Use the equation $g = (g - (g)\theta) + (g)\theta$ for

$g \in G$ to show $G = \ker \theta \oplus \operatorname{im} \theta$. Let $G = \mathbb{Z}_2 \oplus \mathbb{Z}_4$ and let $(\bar{l}, \bar{m})\theta = (\bar{m}, \bar{2}l - m)$ for all $l, m \in \mathbb{Z}$. Show that $\theta : G \rightarrow G$ is idempotent and find generators of $\ker \theta$ and $\operatorname{im} \theta$.

2. (a) Let G and G' be \mathbb{Z} -modules and $\theta : G \rightarrow G'$ a \mathbb{Z} -linear mapping.
 - (i) For each subgroup H of G show that $H' = \{(h)\theta : h \in H\}$ is a subgroup of G' contained in $\operatorname{im} \theta$. Show $H/(\ker \theta \cap H) \cong H'$ by applying Theorem 2.16 to the restriction of θ to H (i.e. the \mathbb{Z} -linear mapping $\theta|_H : H \rightarrow G'$ defined by $(h)\theta|_H = (h)\theta$ for all $h \in H$).
 - (ii) For each subgroup H' of G' , show that $H = \{h \in G : (h)\theta \in H'\}$ is a subgroup of G containing $\ker \theta$. Show $H/\ker \theta \cong H' \cap \operatorname{im} \theta$ by applying Theorem 2.16 to $\theta|_H$.
- (b) The \mathbb{Z} -linear mapping $\theta : \mathbb{Z} \oplus \mathbb{Z} \rightarrow \mathbb{Z}_2$ is defined by $(l, m)\theta = \overline{l - m}$ for all $l, m \in \mathbb{Z}$. Verify that $(1, 1)$ and $(2, 0)$ belong to $\ker \theta$. Show that $(1, 1), (2, 0)$ is a \mathbb{Z} -basis of $\ker \theta$. Show $\operatorname{im} \theta = \mathbb{Z}_2$. Using Theorem 2.16 determine the isomorphism type of $\mathbb{Z} \oplus \mathbb{Z}/\ker \theta$. Use Theorem 2.17 to show that $\ker \theta$ is a maximal subgroup of $\mathbb{Z} \oplus \mathbb{Z}$ (i.e. $\ker \theta \neq \mathbb{Z} \oplus \mathbb{Z}$ and there are no subgroups H of $\mathbb{Z} \oplus \mathbb{Z}$ with $\ker \theta \subset H \subset \mathbb{Z} \oplus \mathbb{Z}$).
- (c) The \mathbb{Z} -linear mapping $\theta : \mathbb{Z} \oplus \mathbb{Z} \rightarrow \mathbb{Z}_4$ is defined by $(l, m)\theta = \overline{l + m}$ for all $l, m \in \mathbb{Z}$. Show that $\ker \theta = \langle (1, -1), (4, 0) \rangle$. Verify that $\operatorname{im} \theta = \mathbb{Z}_4$ and hence find the isomorphism type of $(\mathbb{Z} \oplus \mathbb{Z})/\ker \theta$. List the subgroups H' of \mathbb{Z}_4 and the corresponding subgroups H of $\mathbb{Z} \oplus \mathbb{Z}$ with $\ker \theta \subseteq H$ as in Theorem 2.17. Taking $H' = \langle \bar{2} \rangle$ specify a \mathbb{Z} -basis of the corresponding H .
- (d) The \mathbb{Z} -linear mapping $\theta : \mathbb{Z} \oplus \mathbb{Z} \rightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_4 = G'$ is defined by $(l, m)\theta = (\bar{l}, \bar{m})$ for all $l, m \in \mathbb{Z}$. Verify that $2e_1, 4e_2$ is a \mathbb{Z} -basis of $\ker \theta$. For each of the following subgroups H' of G' specify a \mathbb{Z} -basis ρ_1, ρ_2 of $H = (H')\varphi = \{h \in \mathbb{Z} \oplus \mathbb{Z} : (h)\theta \in H'\}$:

$$\langle (\bar{1}, \bar{0}) \rangle, \quad \langle (\bar{0}, \bar{2}) \rangle, \quad \langle (\bar{1}, \bar{1}) \rangle.$$

In each case find the Smith normal form $\operatorname{diag}(d_1, d_2)$ of the 2×2 matrix $A = \begin{pmatrix} \rho_1 \\ \rho_2 \end{pmatrix}$ and check that G'/H' has isomorphism type $C_{d_1} \oplus C_{d_2}$.

- (e) Let G and G' be \mathbb{Z} -modules and $\theta : G \rightarrow G'$ a surjective \mathbb{Z} -linear mapping. Let H' be a subgroup of G' and $H = \{h \in G : (h)\theta \in H'\}$. By applying Theorem 2.16 to $\theta\eta$, where $\eta : G' \rightarrow G'/H'$ is the natural homomorphism, show $G/H \cong G'/H'$.
3. (a) Let R be a ring with 1-element e . A subgroup K of the additive group of R is called an ideal of R if rk and kr belong to K for all $r \in R, k \in K$. Show that multiplication of cosets is unambiguously defined by $(K + r_1)(K + r_2) = K + r_1r_2$ for all $r_1, r_2 \in R$ (i.e. show that if $K + r_1 = K + r'_1$ and $K + r_2 = K + r'_2$ then $K + r_1r_2 = K + r'_1r'_2$).

Using the notation $K + r = \bar{r}$ and Lemma 2.10, show that the set $R/K = \{\bar{r} : r \in R\}$ of cosets is a ring (*the quotient ring of R by K*). Show further that $\eta : R \rightarrow R/K$, given by $(r)\eta = \bar{r}$ for all $r \in R$, is a ring homomorphism (*the natural homomorphism from R to R/K*). What are $\text{im } \eta$ and $\ker \eta$?

- (b) Let R and R' be rings and let $\theta : R \rightarrow R'$ be a ring homomorphism. Show that $\text{im } \theta$ is a *subring* of R' (i.e. $\text{im } \theta$ is a subgroup of the additive group of R' , $\text{im } \theta$ is closed under multiplication and $\text{im } \theta$ contains the 1-element e' of R').

Show that $K = \ker \theta = \{k \in R : (k)\theta = 0'\}$ is an ideal of R where $0'$ is the 0-element of R' . Prove *the first isomorphism theorem for rings* namely $\tilde{\theta} : R/K \cong \text{im } \theta$ (i.e. $\tilde{\theta}$ defined by $(K + r)\tilde{\theta} = (r)\theta$ for all $r \in R$ is a ring isomorphism).

- (c) Let $\theta : \mathbb{Z} \rightarrow R$ be a ring homomorphism from the ring \mathbb{Z} of integers to a ring R . Use part (b) above and Theorem 1.15 to show that there is a non-negative integer d with $\mathbb{Z}/\langle d \rangle \cong \text{im } \theta$, that is, the rings \mathbb{Z}_d are, up to isomorphism, the (ring) homomorphic images of \mathbb{Z} .
- (d) Let R, R', R'' be rings and let $\theta : R \rightarrow R', \theta' : R' \rightarrow R''$ be ring homomorphisms. Show that $\theta\theta' : R \rightarrow R''$ is a ring homomorphism. Suppose θ is a ring isomorphism. Show that θ^{-1} is also a ring isomorphism. Deduce that the automorphisms θ of R (the ring isomorphisms $\theta : R \rightarrow R$) form a group $\text{Aut } R$, the group operation being mapping composition.

- (e) Let R_1 and R_2 be rings. Show that $R_1 \oplus R_2 = \{(r_1, r_2) : r_1 \in R_1, r_2 \in R_2\}$, with addition and multiplication of ordered pairs defined by $(r_1, r_2) + (r'_1, r'_2) = (r_1 + r'_1, r_2 + r'_2)$, $(r_1, r_2)(r'_1, r'_2) = (r_1 r'_1, r_2 r'_2)$ for all $r_1, r'_1 \in R_1$ and all $r_2, r'_2 \in R_2$, is itself a ring (*the direct sum of R_1 and R_2*).

- (f) Let K and L be ideals of a ring R (see Question 3(a) above). Show that $K \cap L$ and $K + L = \{k + l : k \in K, l \in L\}$ are ideals of R . Establish the *generalised Chinese remainder theorem* which states: suppose $K + L = R$; then $\tilde{\alpha} : R/(K \cap L) \cong R/K \oplus R/L$ is a ring isomorphism where $(r + K \cap L)\tilde{\alpha} = (r + K, r + L)$ for all $r \in R$.

Hint: Consider $\alpha : R \rightarrow R/K \oplus R/L$ defined by $(r)\alpha = (r + K, r + L)$ for all $r \in R$.

4. (a) Let G be a multiplicative group with subgroup K . Then K is called *normal in G* if $g^{-1}kg \in K$ for all $k \in K, g \in G$. Write $Kg = \{kg : k \in K\}$ and $gK = \{gk : k \in K\}$. Show that K is normal in G if and only if $Kg = gK$ for all $g \in G$.

The group S_3 consisting of the 6 bijections (permutations) of $\{1, 2, 3\}$ to $\{1, 2, 3\}$ contains the elements σ and τ where $(1)\sigma = 2, (2)\sigma = 3,$

(3) $\sigma = 1$ and (1) $\tau = 2$, (2) $\tau = 1$, (3) $\tau = 3$. Show that $\langle \sigma \rangle = \{\sigma, \sigma^2, \sigma^3\}$ is normal in S_3 but $\langle \tau \rangle = \{\tau, \tau^2\}$ is not normal in S_3 .

Hint: $\langle \sigma \rangle$ is the subgroup of even permutations in S_3 .

Suppose that K is normal in G . Show that the product of cosets is unambiguously defined by $(Kg_1)(Kg_2) = K(g_1g_2)$ for $g_1, g_2 \in G$. Hence show that the set G/K of all cosets Kg ($g \in G$) is a group, *the quotient group of G by K* – it's the multiplicative version of Lemma 2.10.

- (b) Let $G = U(\mathbb{Z}_{15})$ the multiplicative group of invertible elements in the ring \mathbb{Z}_{15} . List the 8 elements in G . For each of the following subgroups K , partition G into cosets of K , construct the multiplication table of G/K and state the isomorphism type of G/K :

$$K = \{\bar{1}, \bar{4}\}, \quad K = \{\bar{1}, \bar{14}\}, \quad K = \{\bar{1}, \bar{4}, \bar{11}, \bar{14}\}, \\ K = \{\bar{1}, \bar{2}, \bar{4}, \bar{8}\}.$$

From your results decide whether or not (i) $K_1 \cong K_2$ implies $G/K_1 \cong G/K_2$, (ii) $G/K_1 \cong G/K_2$ implies $K_1 \cong K_2$, where K_1 and K_2 are normal subgroups of G .

- (c) Let G and G' be multiplicative groups. Suppose the mapping $\theta : G \rightarrow G'$ satisfies $(g_1g_2)\theta = (g_1)\theta(g_2)\theta$ for all $g_1, g_2 \in G$. Then θ is called a group homomorphism. Show that $(e)\theta = e'$ where e, e' are the identity elements of G, G' by considering $(e^2)\theta$. Deduce that $(g^{-1})\theta = ((g)\theta)^{-1}$ for all $g \in G$.

Show that $K = \ker \theta = \{k \in G : (k)\theta = e'\}$ is a normal subgroup of G . Show that $\text{im } \theta = \{(g)\theta : g \in G\}$ is a subgroup of G' . Prove *the first isomorphism theorem for groups* namely $\tilde{\theta} : G/K \cong \text{im } \theta$, i.e. $\tilde{\theta}$ defined by $(Kg)\tilde{\theta} = (g)\theta$ for all $g \in G$ is a *group isomorphism* (a bijective group homomorphism) – it's the multiplicative version of Theorem 2.16.

Let R be a non-trivial commutative ring and let t be a positive integer. Use Theorem 1.18 to show that $\theta : GL_t(R) \rightarrow U(R)$ given by $(A)\theta = \det A$ for all $A \in GL_t(R)$ is a group homomorphism. Show $\text{im } \theta = U(R)$ and write $\ker \theta = SL_t(R)$ *the special linear group of degree t over R* . Find a formula for $|SL_t(\mathbb{Z}_p)|$ where p is prime.

- (d) Let G_1 and G_2 be multiplicative groups. Show that the Cartesian product $G_1 \times G_2$ (the set of all ordered pairs (g_1, g_2) where $g_1 \in G_1, g_2 \in G_2$) with componentwise multiplication is a group, *the external direct product of G_1 and G_2* – it's the multiplicative version of the external direct sum (Exercises 2.2, Question 4(e)).

The projection homomorphisms $\pi_i : G_1 \times G_2 \rightarrow G_i$ are defined by $(g_1, g_2)\pi_i = g_i$ for all $(g_1, g_2) \in G_1 \times G_2$ where $i = 1, 2$. Show that

$G_1 \times G_2$ has normal subgroups K_1 and K_2 , isomorphic to G_1 and G_2 , such that $K_1 \cap K_2$ is trivial and $K_1 K_2 = \{k_1 k_2 : k_i \in K_i\} = G_1 \times G_2$.

Hint: Use $\ker \pi_i$.

5. (a) Let F be a field with 1-element e . Show that the mapping $\chi : \mathbb{Z} \rightarrow F$, defined by $(m)\chi = me$ for all $m \in \mathbb{Z}$, is a ring homomorphism. The non-negative integer d with $\ker \chi = \langle d \rangle$ is called *the characteristic of F* (d exists by Theorem 1.15). Show that $\tilde{\chi} : \mathbb{Z}_d \cong \text{im } \chi$ (i.e. $\text{im } \chi$ is a subring of F which is isomorphic to \mathbb{Z}_d). Using the fact that F has no divisors of zero, deduce that either $d = 0$ or $d = p$ (prime). It is customary to write $d = \chi(F)$.

Let F be a finite field. Explain why $\mathbb{Z}_p \cong \text{im } \chi$ in this case; $\text{im } \chi = F_0$ is called *the prime subfield of F* . Explain how F has the structure of a vector space over F_0 . Why is this vector space finitely generated? Show $|F| = p^s$ where s is the dimension of F over F_0 . Use the binomial theorem to show $(a + b)^p = a^p + b^p$ for $a, b \in F$. Hence show that $\theta : F \rightarrow F$ defined by $(a)\theta = a^p$ for all $a \in F$ is an automorphism of F (*the Frobenius automorphism*).

- (b) Let d and n be positive integers with $d|n$. Using the notation of Theorem 2.11, let $\delta_1 : \mathbb{Z}_n \rightarrow \mathbb{Z}_d$ be the surjective ring homomorphism given by $(\overline{m}_n)\delta_1 = \overline{m}_d$ for all $m \in \mathbb{Z}$. Let $A = (a_{ij})$ be the $t \times t$ matrix over \mathbb{Z}_n with (i, j) -entry a_{ij} . Write $(A)\delta_t = ((a_{ij})\delta_1)$, i.e. $(A)\delta_t$ is the $t \times t$ matrix over \mathbb{Z}_d with (i, j) -entry $(a_{ij})\delta_1$. Show that $\delta_t : \mathfrak{M}_t(\mathbb{Z}_n) \rightarrow \mathfrak{M}_t(\mathbb{Z}_d)$ is a surjective ring homomorphism. Describe the elements of $\ker \delta_t$ and show $|\ker \delta_t| = (n/d)^{t^2}$.

Take $d = p$ (prime), $n = p^s$ where $s > 0$ and write $\det A = \overline{m}_n$. Show that

$$\begin{aligned} A \in GL_t(\mathbb{Z}_n) &\Leftrightarrow \gcd\{m, p^s\} = 1 \Leftrightarrow \gcd\{m, p\} = 1 \\ &\Leftrightarrow (A)\delta_t \in GL_t(\mathbb{Z}_d). \end{aligned}$$

Deduce that the restriction $\delta_t : GL_t(\mathbb{Z}_n) \rightarrow GL_t(\mathbb{Z}_p)$ is a surjective homomorphism of multiplicative groups having kernel the coset $\ker \delta_t + I$, where I is the $t \times t$ identity matrix over \mathbb{Z}_n . Hence show

$$|GL_t(\mathbb{Z}_{p^s})| = p^{(s-1)t^2} (p^t - 1)(p^t - p) \cdots (p^t - p^{t-1}).$$

Calculate $|GL_3(\mathbb{Z}_4)|$ and $|GL_2(\mathbb{Z}_{17})|$. Does $GL_2(\mathbb{Z}_{125})$ have fewer elements than $GL_2(\mathbb{Z}_{128})$? Taking $p = s = t = 2$, list the 16 matrices in the normal subgroup

$$\ker \delta_2 = \ker \delta_2 + \begin{pmatrix} \overline{1} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix} \text{ of } GL_2(\mathbb{Z}_4).$$

- (c) Let $\alpha : \mathfrak{M}_2(\mathbb{Z}_{72}) \cong \mathfrak{M}_2(\mathbb{Z}_8) \oplus \mathfrak{M}_2(\mathbb{Z}_9)$ be the generalised Chinese remainder theorem isomorphism. Find A_1 and A_2 in $\mathfrak{M}_2(\mathbb{Z}_{72})$ with

$$(A_1)\alpha = \left(\begin{pmatrix} \bar{1} & \bar{2} \\ \bar{3} & \bar{4} \end{pmatrix}, \begin{pmatrix} \bar{5} & \bar{6} \\ \bar{7} & \bar{8} \end{pmatrix} \right),$$

$$(A_2)\alpha = \left(\begin{pmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{pmatrix}, \begin{pmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{0} \end{pmatrix} \right).$$

Calculate $A_1 + A_2$, $A_1 A_2$ and check

$$(A_1 + A_2)\alpha = (A_1)\alpha + (A_2)\alpha, \quad (A_1 A_2)\alpha = (A_1)\alpha(A_2)\alpha.$$

Let $n = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$ where p_1, p_2, \dots, p_k are distinct primes. Write down a formula for $|GL_t(\mathbb{Z}_n)|$ in terms of t , p_i and $q_i = p_i^{s_i}$ for $1 \leq i \leq k$.

6. (a) Let $\rho_1, \rho_2, \dots, \rho_s$ denote the rows of the $s \times t$ matrix A over \mathbb{Z} where $s \leq t$. Show that $\rho_1, \rho_2, \dots, \rho_s$ are \mathbb{Z} -independent elements of \mathbb{Z}^t if and only if all the invariant factors d_1, d_2, \dots, d_s of A are positive. Use Exercises 1.3, Question 5(c) to show that there is a \mathbb{Z} -basis of \mathbb{Z}^t beginning with $\rho_1, \rho_2, \dots, \rho_s$ if and only if $d_1 = d_2 = \cdots = d_s = 1$.
- (b) Let $\rho_1, \rho_2, \dots, \rho_s$ denote the rows of the $s \times t$ matrix A over \mathbb{Z} where $s \geq t$. Let d_1, d_2, \dots, d_t denote the invariant factors of A . Show that $\rho_1, \rho_2, \dots, \rho_s$ generate \mathbb{Z}^t if and only if $d_1 = d_2 = \cdots = d_t = 1$.

Hint: Use Corollaries 1.13 and 1.19.

Suppose $\langle \rho_1, \rho_2, \dots, \rho_s \rangle = \mathbb{Z}^t$ and let $\rho'_1, \rho'_2, \dots, \rho'_t$ denote the rows of A^T . Show that a \mathbb{Z} -basis of \mathbb{Z}^t can be selected from $\rho_1, \rho_2, \dots, \rho_s$ if and only if there are $s - t$ rows of the $s \times s$ identity matrix which together with $\rho'_1, \rho'_2, \dots, \rho'_t$ form a \mathbb{Z} -basis of \mathbb{Z}^s .

Hint: It is possible to select a \mathbb{Z} -basis of \mathbb{Z}^t from $\rho_1, \rho_2, \dots, \rho_s$ if and only if A has a t -minor equal to ± 1 .

- (c) Test each of the following sets for \mathbb{Z} -independence. Which of them is contained in a \mathbb{Z} -basis of \mathbb{Z}^3 ?

$$(i) \quad (1, 3, 2), (4, 6, 5), (7, 9, 8); \quad (ii) \quad (1, 3, 7), (3, 5, 9);$$

$$(iii) \quad (1, 2, 3), (4, 3, 5).$$

Which of the following sets generate \mathbb{Z}^3 ? Which of them contains a \mathbb{Z} -basis of \mathbb{Z}^3 ?

$$(iv) \quad (1, 2, 3), (3, 1, 2), (1, 1, 4), (4, 1, 1);$$

$$(v) \quad (1, 1, 1), (1, 2, 3), (1, 3, 4), (1, 5, 6);$$

$$(vi) \quad (1, 1, 1), (1, 1, 2), (1, 3, 1), (4, 1, 1).$$

7. (a) Let M and M' be R -modules and let $\theta : M \rightarrow M'$ be an R -linear mapping. Suppose that M is free with R -basis v_1, v_2, \dots, v_t . Let $v'_i = (v_i)\theta$ for $1 \leq i \leq t$. Show that v'_1, v'_2, \dots, v'_t generate $M' \Leftrightarrow \theta$ is surjective. Show that v'_1, v'_2, \dots, v'_t are R -independent $\Leftrightarrow \theta$ is injective.
- Let M and M' be free R -modules of rank t and t' respectively. Show that M and M' are isomorphic if and only if $t = t'$.
- (b) Let M be a free R -module of rank t . Suppose u_1, u_2, \dots, u_t generate M . Use Lemma 2.18 and Corollary 2.21 to show that u_1, u_2, \dots, u_t form an R -basis of M .
- (c) Let M and M' be R -modules and let $\theta : M \rightarrow M'$ be an R -linear mapping. Show that $\ker \theta = \{v \in M : (v)\theta = 0\}$ is a submodule of M . Show that $\text{im } \theta = \{(v)\theta : v \in M\}$ is a submodule of M' . Suppose θ is bijective; show that θ^{-1} is R -linear. Is the inverse of an isomorphism of R -modules itself such an isomorphism?
- (d) Let N be a submodule of an R -module M . Complete the proof Lemma 2.27 that M/N is an R -module.
- (e) A non-empty subset N of an R -module M is closed under addition and $ru \in N$ for all $r \in R, u \in N$. Is N a submodule of M ? Justify your answer.
- Let N_1 and N_2 be submodules of an R -module M . Show that $N_1 + N_2 = \{u_1 + u_2 : u_1 \in N_1, u_2 \in N_2\}$ is a submodule of M . Show that $N_1 \cap N_2$ is a submodule of M .
- (f) Let M_1 and M_2 be R -modules. Using Exercises 2.2, Question 4(f) show that the Cartesian product

$$M_1 \times M_2 = \{(v_1, v_2) : v_1 \in M_1, v_2 \in M_2\}$$

is an R -module (the external direct sum $M_1 \oplus M_2$ of M_1 and M_2) on defining $(v_1, v_2) + (v'_1, v'_2) = (v_1 + v'_1, v_2 + v'_2)$ and $r(v_1, v_2) = (rv_1, rv_2)$ for all $v_1, v'_1 \in M_1, v_2, v'_2 \in M_2, r \in R$.

Use (e) above to show that $N_1 = \{(v_1, 0) \in M_1 \oplus M_2\}$ and $N_2 = \{(0, v_2) \in M_1 \oplus M_2\}$ are submodules of $M_1 \oplus M_2$ satisfying $N_1 + N_2 = M_1 \oplus M_2, N_1 \cap N_2 = \{(0, 0)\}$. Show that there are R -linear isomorphisms $\alpha_1 : N_1 \cong M_1$, and $\alpha_2 : N_2 \cong M_2$.

What is the connection between the external direct sum $M_1 \oplus M_2$ and the internal direct sum $N_1 \oplus N_2$? (The answer is very short!)



<http://www.springer.com/978-1-4471-2729-1>

Finitely Generated Abelian Groups and Similarity of
Matrices over a Field

Norman, C.

2012, XII, 381 p., Softcover

ISBN: 978-1-4471-2729-1