0.3 Abelian groups

The goal of this section is to look at several properties of abelian groups and see how they relate to general properties of modules. I'll usually repeat the definitions I've already given for modules, to keep this section more or less independent of the previous one. We first need to write down the definition of a group. To shorten it a bit, we use the definition that a *binary operation* is one in which the closure property holds.

DEFINITION 0.3.1. A *group* is a nonempty set G with a binary operation $\cdot$ defined on G such that the following conditions hold:

(i) for all $a, b, c \in G$, we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c$;

(ii) there exists an element $1 \in G$ such that $1 \cdot a = a$ and $a \cdot 1 = a$ for all $a \in G$;

(iii) for each $a \in G$ there exists an element $a^{-1} \in G$ such that $a \cdot a^{-1} = 1$ and $a^{-1} \cdot a = 1$.

DEFINITION 0.3.2. The group G is said to be *abelian* if $a \cdot b = b \cdot a$ for all $a, b \in G$.

If the group G is abelian, it is customary to denote the operation additively, using a $+$ symbol, and to use the symbol 0 for the identity element. Using additive notation, we can rewrite the axioms for an abelian group in a way that points out the similarities with vector spaces and fields.

An abelian group is a nonempty set A with a binary operation $+$ defined on A such that the following conditions hold:

(i) (*Associativity*) for all $a, b, c \in A$, we have $a + (b + c) = (a + b) + c$;

(ii) (*Commutativity*) for all $a, b \in A$, we have $a + b = b + a$;

(iii) (*Existence of an additive identity*) there exists an element $0 \in A$ such that $0 + a = a$ for all $a \in A$;

(iv) (*Existence of additive inverses*) for each $a \in A$ there exists an element $-a \in A$ such that $-a + a = 0$.

You should notice that any field is an abelian group under addition. Furthermore, under multiplication, the set of nonzero elements of any field must also form an abelian group. Of course, in this case the two operations are not independent–they are connected by the distributive laws.

The definition of an abelian group is also useful in discussing vector spaces and modules. In fact, we can define a vector space to be an abelian group together with a scalar multiplication satisfying the relevant axioms. Using this definition of a vector space as a model, we can state the definition of a module in the following way.

DEFINITION 0.3.3. A *left module* over the ring R is an abelian group M, together with a scalar multiplication $\cdot$ defined on M such that the following conditions hold:

(i) $a \cdot x \in M$;

(ii) $a \cdot (b \cdot x) = (ab) \cdot x$;

(iii) $(a + b) \cdot x = a \cdot x + b \cdot x$;

(iv) $a \cdot (x + y) = a \cdot x + a \cdot y$;
(v) $1 \cdot x = x$;
for all $a, b \in R$ and all $x, y \in M$.

But the point of this section is to look at abelian groups that don't have a given module structure. I'm sure that soon after you first met the definition of a group you started to use the shorthand notation $a + a = 2a$, $a + a + a = 3a$, and so on, for any element a in any abelian group. When the inverse of a is involved, we can write $(-a) + (-a) = -2a$, etc. If we also agree that $0a = 0$, then we really have a "scalar multiplication" in which the scalars come from the ring $\mathbf{Z}$ of integers. The whole point is that this "multiplication" already comes built into the addition defined on the group. You should check all of the necessary axioms, to make sure you understand why the next proposition is true.

PROPOSITION 0.3.4. Every abelian group has a natural structure as a module over the ring $\mathbf{Z}$.

As with vector spaces, one goal is to be able to express an abelian group in terms of simpler building blocks. For vector spaces we can use one-dimensional spaces as the building blocks; for abelian groups, it seems natural to use the *simple* abelian groups.

Recall that in an arbitrary group G, a subgroup $N \subseteq G$ is called a *normal subgroup* if $gxg^{-1} \in N$, for all $x \in N$ and all $g \in G$. Then G is said to be a *simple group* if its only normal subgroups are $\{1\}$ and G. If the group A is abelian, then all subgroups are normal, and so A is simple iff its only subgroups are the trivial subgroup (0) and the improper subgroup A. The same definition is given for modules: a nonzero module M is a *simple module* if its only submodules are (0) and M. When you view an abelian group as a $\mathbf{Z}$-module, then, of course, the two definitions coincide.

Compared to the classification of *all* simple groups, it is absolutely trivial to give a complete classification of all simple *abelian* groups. Even though I certainly hope that you remember the proof, I've decided to outline it anyway.

LEMMA 0.3.5. Any cyclic abelian group is isomorphic to $\mathbf{Z}$ or $\mathbf{Z}_n$, for some n.

Outline of the proof: Let A be a cyclic abelian group that is generated by the single element a. Define the group homomorphism $f : \mathbf{Z} \to A$ by setting $f(n) = na$, for all $n \in \mathbf{Z}$. Note that f maps $\mathbf{Z}$ onto A since $f(\mathbf{Z}) = \mathbf{Z}a = A$. If f is one-to-one, then A is isomorphic to $\mathbf{Z}$. If f is not one-to-one, we need to use the fundamental homomorphism theorem (Theorem 1.2.7) and the fact that every subgroup of $\mathbf{Z}$ is cyclic to show that A is isomorphic to $\mathbf{Z}_n$, where n is the smallest positive integer such that $na = 0$. □

PROPOSITION 0.3.6. An abelian group is simple iff it is isomorphic to $\mathbf{Z}_p$, for some prime number p.

Proof: First, let A be an abelian group isomorphic to $\mathbf{Z}_p$, where p is a prime number. The isomorphism preserves the subgroup structure, so we only need to know that $\mathbf{Z}_p$ has no proper nontrivial subgroups. This follows from the general correspondence between

subgroups of $\mathbf{Z}_n$ and divisors of n, since p is prime precisely when its only divisors are ± 1 and $\pm p$, which correspond to the subgroups $\mathbf{Z}_p$ and (0), respectively.

Conversely, suppose that A is a simple abelian group. Since A is nonzero, pick any nonzero element $a \in A$. Then the set $\mathbf{Z}a = \{na \mid n \in \mathbf{Z}\}$ is a nonzero subgroup of A, so by assumption it must be equal to A. This shows that A is a cyclic group. Furthermore, A can't be infinite, since then it would be isomorphic to $\mathbf{Z}$ and would have infinitely many subgroups. We conclude that A is finite, and hence isomorphic to $\mathbf{Z}_n$, for some n. Once again, the correspondence between subgroups of $\mathbf{Z}_n$ and divisors of n shows that if $\mathbf{Z}_n$ is simple, then n must be a prime number. □

A module M is said to be *semisimple* if it can be expressed as a sum (possibly infinite) of simple submodules (see Definition 2.3.1 (b)). Although the situation for abelian groups is more complicated than for vector spaces, it is natural to ask whether all abelian groups are semisimple. This isn't true, as the next example shows. That makes it interesting to try to find out which abelian groups actually *are* semisimple.

EXAMPLE 0.3.1. The group $\mathbf{Z}_4$ is not a semisimple $\mathbf{Z}$-module. First, $\mathbf{Z}_4$ is not a simple group. Secondly, it cannot be written nontrivially as a direct sum of any subgroups, since its subgroups lie in a chain $\mathbf{Z}_4 \supset 2\mathbf{Z}_4 \supset (0)$, and no two proper nonzero subgroups intersect in (0).

EXAMPLE 0.3.2. The group $\mathbf{Z}_6$ is a semisimple $\mathbf{Z}$-module. To see this, define $f : \mathbf{Z}_6 \to \mathbf{Z}_2 \oplus \mathbf{Z}_3$ by setting $f(0) = (0,0)$, $f(1) = (1,1)$, $f(2) = (0,2)$, $f(3) = (1,0)$, $f(4) = (0,1)$, $f(5) = (1,2)$. You can check that this defines an isomorphism, showing that $\mathbf{Z}_6$ is isomorphic to a direct sum of simple abelian groups.

Exercise 2.3.2 in the text asks you to classify all finite semisimple abelian groups, and the previous example should give you a big hint. The function defined in the example is a special case of a more general result that is usually referred to as the Chinese remainder theorem (this result is given more generally for rings, in Theorem 1.2.12). The proof of the next proposition makes use of the same function.

PROPOSITION 0.3.7. If $k = mn$, where m and n are relatively prime integers, then $\mathbf{Z}_k$ is isomorphic to $\mathbf{Z}_m \oplus \mathbf{Z}_n$.

Outline of the proof: Define $f : \mathbf{Z}_k \to \mathbf{Z}_m \oplus \mathbf{Z}_n$ by $f([x]_k) = ([x]_m, [x]_n)$, for all $x \in \mathbf{Z}$. Here I have been a bit more careful, by using $[x]_k$ to denote the congruence class of x, modulo k. It is not hard to show that f preserves addition. The sets $\mathbf{Z}_k$ and $\mathbf{Z}_m \oplus \mathbf{Z}_n$ are finite and have the same number of elements, so f is one-to-one iff it is onto, and therefore proving one of these conditions will give the other. (Actually, it isn't hard to see how to prove both conditions.) Showing that f is one-to-one depends on the fact that if x is an integer having both m and n as factors, then it must have mn as a factor since m and n are relatively prime. On the other hand, the usual statement of the Chinese remainder theorem is precisely the condition that f is an onto function. □

COROLLARY 0.3.8. Any finite cyclic group is isomorphic to a direct sum of cyclic groups of prime power order.

I have to admit that the corollary depends on an important result in $\mathbf{Z}$: every positive integer can be factored into a product of prime numbers. Grouping the primes together, the proof of the corollary uses induction on the number of distinct primes in the factorization.

This basic result has implications for all finite groups. The cyclic group $\mathbf{Z}_n$ also has a ring structure, and the isomorphism that proves the corollary is actually an isomorphism of rings, not just of abelian groups. To use this observation, suppose that A is a finite abelian group. Let n be the smallest positive integer such that $na = 0$ for all $a \in A$. (This number might be familiar to you in reference to a multiplicative group G, where it is called the *exponent* of the group, and is the smallest positive integer n such that $g^n = 1$ for all $g \in G$.) For the additive group A, we usually refer to $n\mathbf{Z}$ as the *annihilator* of A. You can check that because $na = 0$ for all $a \in A$, we can actually give A the structure of a $\mathbf{Z}_n$-module.

Next we can apply a general result (Proposition 2.2.7) that says that if a ring R can be written as a direct sum $R = I_1 \oplus \cdots \oplus I_n$ of two-sided ideals, then each I_j is a ring in its own right, and every left R-module M splits up into a direct sum $M_1 \oplus \cdots \oplus M_n$, where M_j is a module over I_j. Applying this to $\mathbf{Z}_n$, we can write $\mathbf{Z}_n$ as a direct sum of rings of the form $\mathbf{Z}_{p^k}$, where p is a prime, and then the group A breaks up into $A_1 \oplus \cdots \oplus A_n$, where each A_j is a p-group, for some prime p. (Recall that a group G is a p-group if every element of G has order p.) This argument proves the next lemma. (You can also prove it using Sylow subgroups, if you know about them.)

LEMMA 0.3.9. Every abelian group can be written as a direct sum of p-groups.

The decomposition into p-groups occurs in one and only one way. Then it is possible to prove that each of the p-groups splits up into cyclic groups of prime power order, and so we have the following fundamental structure theorem for finite abelian groups.

THEOREM 0.3.10. Any finite abelian group is isomorphic to a direct sum of cyclic groups of prime power order.

I will end the section with a proof of the fundamental structure theorem, but I want to first discuss some of the directions it suggests for module theory. First of all, the hope was to construct finite abelian groups out of ones of *prime* order, not prime *power* order. The only way to do this is to stack them on top of each other, instead of having a direct sum in which the simple groups are lined up one beside the other. To see what I mean by "stacking" the groups, think of $\mathbf{Z}_4$ and its subgroups $\mathbf{Z}_4 \supset 2\mathbf{Z}_4 \supset (0)$. It might be better to picture them vertically.

$$\begin{array}{c} \mathbf{Z}_4 \\ | \\ 2\mathbf{Z}_4 \\ | \\ (0) \end{array}$$

The subgroup $2\mathbf{Z}_4 = \{0, 2\} \cong \mathbf{Z}_2$ is simple, and so is the factor module $\mathbf{Z}_4/2\mathbf{Z}_4 \cong \mathbf{Z}_2$. I think of this as having $\mathbf{Z}_2$ stacked on top of $\mathbf{Z}_2$, and the group is structured so tightly that you can't even find an isomorphism to rearrange the factors.

In Definition 2.5.1, a module M is said to have a *composition series* of length n if there is a chain of submodules $M = M_0 \supset M_1 \supset \cdots \supset M_n = (0)$ for which each factor module M_{i-1}/M_i is a simple module. Thus we would say that $\mathbf{Z}_4$ has a composition series of length 2. This gives a measurement that equals the dimension, in the case of a vector space. It is also true that the length of a cyclic group of order p^n is precisely n. It can be shown (Theorem 2.5.2) that if M has a composition series of length n, then every other composition series also has length n, so this is an invariant of the module. Furthermore, the same simple modules show up in both series, with the same multiplicity.

The idea of a composition series is related to two other conditions on modules. A module is said to satisfy the *ascending chain condition*, or ACC, if it has no infinite chain of ascending submodules; it is said to satisfy the *descending chain condition*, or DCC, if it has no infinite chain of descending submodules. Modules satisfying these conditions are called *Noetherian* or *Artinian*, respectively. Proposition 2.5.4 shows that a module has finite length iff it satisfies both the ACC and DCC. As an example to keep in mind, let's look at the ring of integers, which has has ACC but not DCC. Since $m\mathbf{Z} \subseteq n\mathbf{Z}$ iff $n \mid m$, generators get smaller as you go up in $\mathbf{Z}$, and larger as you go down. Any set of positive integers has a smallest element, so we can't have any infinite ascending chains, but, for example, we can construct the infinite descending chain $2\mathbf{Z} \supset 4\mathbf{Z} \supset 8\mathbf{Z} \supset \cdots$.

The cyclic groups of prime power order play a crucial role in the structure of finite abelian groups precisely because they cannot be split up any further. A module M can be expressed as a direct sum of two submodules M_1 and M_2 iff $M_1 \cap M_2 = (0)$ and $M_1 + M_2 = M$. In the case of a cyclic group of prime power order, the subgroups form a descending chain, and so any two nonzero subgroups have a nonzero intersection. In Definition 2.5.5, a module is called *indecomposable* if it cannot be written as a direct sum of two nonzero submodules. With this terminology, the cyclic groups of prime power order are precisely the indecomposable abelian groups. The major results in this direction are Proposition 2.5.6 and Theorem 2.5.11 (the Krull-Schmidt theorem), which show that any module with finite length can be written as a direct sum of indecomposable submodules, and this decomposition is unique up to isomorphism and the order of the summands.

After this rather lengthy preview, or review, as the case may be, it is time to move on to study general rings and modules. The next results present a proof of the structure theorem for finite abelian groups, but you should feel free to skip them. You might want to come back to this proof later, to compare it with the proof given in Section 2.7, where we will prove the structure theorem for finitely generated modules over a principal ideal domain.

LEMMA 0.3.11. Let A be a finite abelian p-group.

(a) Let $a \in A$ be an element of maximal order, and let $b + \mathbf{Z}a$ be any coset of $A/\mathbf{Z}a$. Then there exists $d \in A$ such that $d + \mathbf{Z}a = b + \mathbf{Z}a$ and $\mathbf{Z}d \cap \mathbf{Z}a = (0)$.

(b) Let $a \in A$ be an element of maximal order. Then there exists a subgroup B with $A \cong \mathbf{Z}a \oplus B$.

Proof: (a) *The outline of part (a) is to let s be the smallest positive integer such that $sb \in \mathbf{Z}a$. Then we solve the equation $sb = sx$ for elements $x \in \mathbf{Z}a$ and let $d = b - x$.*

Using $o(x)$ for the order of an element x, let s be the order of $b + \mathbf{Z}a$ in the factor group $G/\mathbf{Z}a$. Then $sb \in \mathbf{Z}a$, and we can write $sb = (qt)a$ for some exponent qt such that $t = p^\beta$ for some β and $p \nmid q$. Then qa is a generator for $\mathbf{Z}a$, since q is relatively prime to $o(a)$. Since s is a divisor of the order of b, we have $o(b)/s = o(sb) = o((qt)a) = o(a)/t$, or simply, $o(b) \cdot t = o(a) \cdot s$. All of these are powers of p, and so $o(b) \leq o(a)$ implies that $s|t$, say $t = ms$. Then $x = (qm)a$ is a solution of the equation $sb = sx$. If $d = b - x$, then $d + \mathbf{Z}a = b + \mathbf{Z}a$ and so $sd = sb - sx = sb - sb = 0$. Therefore $\mathbf{Z}d \cap \mathbf{Z}a = (0)$, since $nd \in \mathbf{Z}a$ implies $n(b - x) = nb - nx \in \mathbf{Z}a$. Thus $nb \in \mathbf{Z}a$ implies $n(b + \mathbf{Z}a) = \mathbf{Z}a$ in $G/\mathbf{Z}a$, so $s|n$ and $nd = 0$.

(b) *The outline of this part is to factor out $\mathbf{Z}a$ and use induction to decompose $A/\mathbf{Z}a$ into a direct sum of cyclic groups. Then part (a) can be used to choose the right preimages of the generators of $A/\mathbf{Z}a$ to generate the complement B of $\mathbf{Z}a$.*

We use induction on the order of A. If $|A|$ is prime, then A is cyclic and there is nothing to prove. Consequently, we may assume that the statement of the lemma holds for all groups of order less than $|A| = p^\alpha$. If A is cyclic, then we are done. If not, let $\mathbf{Z}a$ be a maximal cyclic subgroup, and use the induction hypothesis repeatedly to write $A/\mathbf{Z}a$ as a direct sum $B_1 \oplus B_2 \oplus \cdots \oplus B_n$ of cyclic subgroups.

We next use part (a) to choose, for each i, a coset $a_i + \mathbf{Z}a$ that corresponds to a generator of A_i such that $\mathbf{Z}a_i \cap \mathbf{Z}a = (0)$. We claim that $A \cong \mathbf{Z}a \oplus B$ for the smallest subgroup $B = \mathbf{Z}a_1 + \mathbf{Z}a_2 + \cdots + \mathbf{Z}a_n$ that contains a_1, a_2, ..., a_n.

First, if $x \in \mathbf{Z}a \cap (\mathbf{Z}a_1 + \cdots + \mathbf{Z}a_n)$, then $x = m_1a_1 + \cdots + m_na_n \in \mathbf{Z}a$ for some coefficients $m_1, \ldots, m_n$. Thus $x + \mathbf{Z}a = (m_1a_1 + \cdots + m_na_n) + \mathbf{Z}a = \mathbf{Z}a$, and since $A/\mathbf{Z}a$ is a direct sum, this implies that $m_ia_i + \mathbf{Z}a = \mathbf{Z}a$ for each i. But then $m_ia_i \in \mathbf{Z}a$, and so $m_ia_i = 0$ since $\mathbf{Z}a_i \cap \mathbf{Z}a = (0)$. Thus $x = 0$.

Next, given $x \in A$, express the coset $x + \mathbf{Z}a$ as $(m_1a_1 + \cdots + m_na_n) + \mathbf{Z}a$ for coefficients m_1, ..., m_n. Then $x \in x\mathbf{Z}a$, and so $x = ma + m_1a_1 + \cdots + m_na_n$ for some m.

Thus we have shown that $\mathbf{Z}a \cap B = (0)$ and $A = \mathbf{Z}a + B$, so $A \cong \mathbf{Z}a \oplus B$. □

THEOREM 0.3.12. (Fundamental Theorem of Finite Abelian Groups) Any finite abelian group is isomorphic to a direct sum of cyclic groups of prime power order. Any two such decompositions have the same number of factors of each order.

Proof: We first decompose any abelian group A into a direct sum of p-groups, and then we can use the previous lemma to write each of these groups as a direct sum of cyclic subgroups.

Uniqueness is shown by induction on $|A|$. It is enough to prove the uniqueness for a given p-group. Suppose that

$$\mathbf{Z}_{p^{\alpha_1}} \oplus \mathbf{Z}_{p^{\alpha_2}} \oplus \cdots \oplus \mathbf{Z}_{p^{\alpha_n}} = \mathbf{Z}_{p^{\beta_1}} \oplus \mathbf{Z}_{p^{\beta_2}} \oplus \cdots \oplus \mathbf{Z}_{p^{\beta_m}}$$

where $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_n$ and $\beta_1 \geq \beta_2 \geq \ldots \geq \beta_m$. Consider the subgroups in which each element has been multiplied by p. By induction, $\alpha_1 - 1 = \beta_1 - 1$, ..., which gives $\alpha_1 = \beta_1$, ..., with the possible exception of the α_i's and β_j's that equal 1. But the groups have the

same order, and this determines that each has the same number of factors isomorphic to $\mathbf{Z}_p$. This completes the proof. □

EXERCISES

1. If any facts in this section on abelian groups caused you problems, you should review your elementary group theory.
2. You don't have to review it now, but make sure you have a reference book that has some elementary linear algebra.