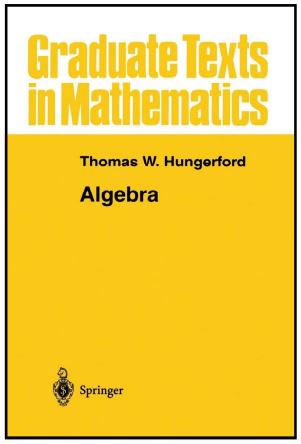
Modern Algebra

Chapter II. The Structure of Groups

II.1. Free Abelian Groups—Proofs of Theorems



Theorem II.1.1

Theorem II.1.1. The following conditions on an abelian group F are equivalent.

- (i) F has a nonempty basis.
- (ii) F is the (internal) direct sum of a family of infinite cyclic subgroups.
- (iii) F is (isomorphic to) a direct sum of copies of the additive group $\mathbb{Z}$ of integers.
- (iv) There exists a nonempty set X and a function $\iota : X \to F$ with the following property: Given an abelian group G and function $f : X \to G$, there exists a unique homomorphism of groups $\overline{f} : F \to G$ such that $\overline{f}\iota = f$. In other words, F is a free object in the category of abelian groups.

Proof. $(i) \Rightarrow (ii)$ If X is a basis of F, then for each $x \in X$, $nx = 0$ if and only if $n = 0$.

Theorem II.1.1 (continued 1)

Theorem II.1.1. The following conditions on an abelian group F are equivalent.

- (i) F has a nonempty basis.
- (ii) F is the (internal) direct sum of a family of infinite cyclic subgroups.

Proof (continued). Hence, each subgroup $\langle x \rangle$, where $x \in X$, is an infinite cyclic group (and since F is abelian, therefore a normal subgroup of F). Since F is generated by X, $F = \langle X \rangle$, then $F = \langle \cup_{x \in X} \langle x \rangle \rangle$ (since $\cup_{x \in X} \langle x \rangle$ is simply the set of all "multiples" of $x \in X$). ASSUME for some $z \in X$, $\langle z \rangle \cap (\cup_{x \in X, x \neq z} \langle x \rangle) \neq \{0\}$, then for some nonzero $n \in \mathbb{Z}$ and some distinct $x_1, x_2, \ldots, x_k \in X$ we have $nz = n_1 x_1 + n_2 x_2 + \cdots + n_k x_k$. But then we have distinct $z, x_1, x_2, \ldots, x_k \in X$ such that $n_1 x_1 + n_2 x_2 + \cdots + n_k x_k + (-n)z = 0$ where $-n \neq 0$, CONTRADICTING the definition of basis. So the assumption is false and it must be that $\langle z \rangle \cap (\cup_{x \in X, x \neq z} \langle x \rangle) = \{0\}$. By Definition I.8.8, F is the internal direct sum $F = \sum_{x \in X} \langle x \rangle$. $\square$

Theorem II.1.1 (continued 2)

Theorem II.1.1. The following conditions on an abelian group F are equivalent.

- (ii) F is the (internal) direct sum of a family of infinite cyclic subgroups.
- (iii) F is (isomorphic to) a direct sum of copies of the additive group $\mathbb{Z}$ of integers.

Proof (continued). $(ii) \Rightarrow (iii)$ Suppose F is the (internal) direct sum of a family of infinite cyclic subgroups. By Theorem I.3.2, an infinite cyclic group is isomorphic to $\mathbb{Z}$. Let I be the indexing set for the direct sum. Then by the definition of internal direct sum (Definition I.8.8), $F \cong \sum_{i \in I}^{w} C_i$ (as given in Theorem I.8.6) where each C_i is an infinite cyclic group. Since each C_i is isomorphic to $\mathbb{Z}$ then by Theorem I.8.10 F is isomorphic to a direct sum of copies of $\mathbb{Z}$. $\square$

Theorem II.1.1 (continued 3)

Theorem II.1.1. The following conditions on an abelian group F are equivalent.

(i) F has a nonempty basis.

(iii) F is (isomorphic to) a direct sum of copies of the additive group $\mathbb{Z}$ of integers.

Proof (continued). $(iii) \Rightarrow (i)$ Suppose $F \cong \sum_{x \in X} \mathbb{Z}$. For each $x \in X$, let θ_x be the element of F, $\theta_x = \{u_i\}$, where $u_i = 0$ for $i \neq x$ and $u_i = 1$ for $i = x$. Now for any $z \in \sum \mathbb{Z}_x$, since $\sum \mathbb{Z}$ is abelian and so each $\mathbb{Z}_x$ is isomorphic to a normal subgroup of F, then by Theorem I.8.9 z is a unique finite sum of (images under the isomorphism of) elements of the $\mathbb{Z}_x$'s and each element of $\mathbb{Z}_x$ is a multiple of $1 \in \mathbb{Z}_x$, so z can be written as a finite sum of the θ_x's. So $\{\theta_x \mid x \in X\}$ is a generating set of $\sum \mathbb{Z}_x$.

Theorem II.1.1 (continued 4)

Theorem II.1.1. The following conditions on an abelian group F are equivalent.

(i) F has a nonempty basis.

(iii) F is (isomorphic to) a direct sum of copies of the additive group $\mathbb{Z}$ of integers.

Proof (continued). Now if $x_1, x_2, \ldots, x_k \in X$ are distinct and $n_i \in \mathbb{Z}$ then $n_1 x_1 + n_2 x_2 + \cdots + n_k x_k = 0$ implies $n_1 \theta_{x_1} = n_2 \theta_{x_2} = \cdots = n_k \theta_{x_k} = 0$ (since the x_i are distinct and "0" represents $\{u_i\} \in \sum \mathbb{Z}_x$ with $u_i = 0$ for all $x \in X$). That is, $n_1 = n_2 = \cdots = n_k = 0$. So in fact $\{\theta_x \mid x \in X\}$ is a basis for $\sum \mathbb{Z}$. Since $\sum \mathbb{Z} \cong F$, say with isomorphism f, then $\{f(\theta_x) \mid x \in X\}$ is a basis for F. $\square$

Theorem II.1.1 (continued 5)

Theorem II.1.1. The following conditions on an abelian group F are equivalent.

(i) F has a nonempty basis.

(iv) There exists a nonempty set X and a function $\iota : X \to F$ with the following property: Given an abelian group G and function $f : X \to G$, there exists a unique homomorphism of groups $\overline{f} : F \to G$ such that $\overline{f}\iota = f$. In other words, F is a free object in the category of abelian groups.

Proof (continued). $(i) \Rightarrow (iv)$ Let X be a basis of F and $\iota : X \to F$ be the inclusion map. Suppose we are given a map $f : X \to G$. If $u \in F$ then $u = n_1 x_1 + n_2 x_2 + \cdots + n_k x_k$ for some $n_i \in \mathbb{Z}$ and $x_i \in X$ since X is a basis of F. If $u = m_1 x_1 + m_2 x_2 + \cdots + m_k x_k$ also (with $m_i \in \mathbb{Z}$), then $\sum_{i=1}^k (n_i - m_i) x_i = 0$ and so $n_i = m_i$ since X is a basis of F.

Theorem II.1.1 (continued 6)

Proof (continued). Define the map $\overline{f} : F \to G$ as

$$\overline{f}(u) = \overline{f}\left(\sum_{i=1}^k n_i x_i\right) = n_1 f(x_1) + n_2 f(x_2) + \cdots + n_k f(x_k).$$

Then $\overline{f}$ is well-defined (i.e., independent of the representation of u in terms of elements of X, since this representation is unique). Also, $\overline{f}\iota : X \to G$ is the same as $f : X \to G$. Since G is abelian then for $u, v \in F$ with $u = \sum n_i x_i$ and $v = \sum m_i x_i$ for $n_i, m_i \in \mathbb{Z}$ (some of the n_i, m_i may have to be 0 to get "common" x_i's)

$$\begin{aligned}
\overline{f}(u+v) &= \overline{f}\left(\sum n_i x_i + \sum m_i x_i\right) \\
&= \overline{f}\left(\sum (n_i + m_i) x_i\right) \text{ since } F \text{ is abelian} \\
&= \sum (n_i + m_i) f(x_i) \\
&= \sum n_i f(x_i) + \sum m_i f(x_i) \text{ since } G \text{ is abelian}
\end{aligned}$$

Theorem II.1.1 (continued 7)

Proof (continued).

$$\begin{aligned}\overline{f}(u+v) &= \sum n_i f(x_i) + \sum m_i f(x_i) \text{ since } G \text{ is abelian}\\ &= \overline{f}(u) + \overline{f}(v),\end{aligned}$$

so $\overline{f}$ is a homomorphism. Since X generates F, any homomorphism $F \to G$ is completely determined by its action on X. Thus if $g : F \to G$ is a homomorphism such that $g\iota = f$ (so $g\iota$ is defined on X) then for any $x \in X$ we have $g(x) = g(\iota(x)) = f(x) = \overline{f}(x)$ "whence" $g = \overline{f}$ on X (and ergo on F) and $\overline{f}$ is a unique homomorphism such that $\overline{f}\iota = f$, as claimed. That is, F is a free object on the set X (see Definition I.7.7) in the category of abelian groups. □

Theorem II.1.1 (continued 8)

Theorem II.1.1. The following conditions on an abelian group F are equivalent.

(iii) F is (isomorphic to) a direct sum of copies of the additive group $\mathbb{Z}$ of integers.

(iv) There exists a nonempty set X and a function $\iota : X \to F$ with the following property: Given an abelian group G and function $f : X \to G$, there exists a unique homomorphism of groups $\overline{f} : F \to G$ such that $\overline{f}\iota = f$. In other words, F is a free object in the category of abelian groups.

Proof (continued). $(iv) \Rightarrow (iii)$ Given $\iota : X \to F$, construct the direct sum $\sum \mathbb{Z}$ with the copies of $\mathbb{Z}$ indexed by X. Let $Y = \{\theta_x \mid x \in X\}$ be the basis of $\sum \mathbb{Z}$ as in the proof of $(iii) \Rightarrow (i)$ (the "standard basis"). The proof of $(iii) \Rightarrow (i) \Rightarrow (iv)$ (with $F = \sum \mathbb{Z}$) shows that $\sum \mathbb{Z}$ is a free object on set Y. Since Y is indexed by set X then $|X| = |Y|$ and so by Theorem I.7.8 F is equivalent to F'. The category is abelian groups, so equivalence is group isomorphism. So $F \cong \sum \mathbb{Z}$. □

Theorem II.1.2

Theorem II.1.2. Any two bases of a free abelian group F have the same cardinality.

Proof. First suppose F has a basis X of finite cardinality n so that $F \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ (n summands; by the proof of Theorem II.1.1 where $\{\theta_x \mid x \in X\} = \{(1,0,0,\ldots,0),(0,1,0,\ldots,0),(0,0,\ldots,0,1)\}$). For any subgroup G of F we have that $2G = \{2u \mid u \in G\}$ is a subgroup of G (we just need to show closure of $2G$ which is fairly clear). Now the restriction of the isomorphism between F and $\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ to $2F$ is an isomorphism between $2F$ and $2\mathbb{Z} \oplus 2\mathbb{Z} \oplus \cdots \oplus 2\mathbb{Z}$ (since, say, $\pi(2f_1) = \pi(f_1 + f_1) = \pi(f_1) + \pi(f_1) = 2\pi(f_1)$). Since all groups are abelian, then all subgroups are normal and by Corollary I.8.11 we have $F/2F \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$ (with n summands). Therefore $|F/2F| = |\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2| = 2^n$.

Theorem II.1.2 (continued 1)

Theorem II.1.2. Any two bases of a free abelian group F have the same cardinality.

Proof (continued). If Y is another basis of F and $r \in \mathbb{Z}$ such that $|Y| \geq r$, then we can repeat the argument above to show that (again using the basis from the proof of Theorem II.1.1) $|F/2F| \geq 2^r$, whence $2^r \leq 2^n$ and so $r \leq n$. It follows that $|Y| = m \leq n$ and (as above) $|F/2F| = 2^m$. Therefore $2^m = 2^n$ and $|X| = n = m = |Y|$. (And similarly if $|Y| \leq r$ we get $|X| = |Y|$.) So the result holds for finite bases.
If one basis of F is infinite, then all bases are infinite by the previous paragraph (we have shown that if one basis if finite then another is finite, so we are quoting the contrapositive here). So if we can show that $|X| = |F|$ for any infinite basis, then this suffices. Since $X \subseteq F$ then $|X| \leq |F|$ (see Definition 0.8.4).

Theorem II.1.2 (continued 2)

Theorem II.1.2. Any two bases of a free abelian group F have the same cardinality.

Proof (continued). Let $S = \cup_{n\in\mathbb{N}} X^n$ where $X^n = X \times X \times \cdots \times X$ (n factors). For each $s = (x_1, x_2, \ldots, x_n) \in S$, let G_s be the subgroup $\langle x_1, x_2, \ldots, x_n\rangle$. Then $G_s \cong \mathbb{Z}y_1 \oplus \mathbb{Z}y_2 \oplus \cdots \oplus \mathbb{Z}y_t$ (see the note after Theorem II.1.1; $\langle x\rangle$ is denoted $\mathbb{Z}x$) where $y_1, y_2, \ldots y_t$ are the distinct elements of $\{x_1, x_2, \ldots, x_n\}$. Therefore in terms of cardinality, $|G_2| = |\mathbb{Z}^t| = |\mathbb{Z}| = \aleph_0$ by Theorem 0.8.12. Since X is a basis of F then $F = \cup_{s\in S} G_s$ and so $|F| = |\cup_{s\in S} G_s| \leq |S|\aleph_0$ by Exercise 0.8.12. But by Theorem 0.8.11, $|S|\aleph_0 = |S|$ (since $|S| \geq \aleph_0$) and by Theorem 0.8.12(ii) $|S| = |\cup_{n\in\mathbb{N}} X^n| = \aleph_0|X| = |X|$. So $|F| \leq |S|\aleph_0 = |S| = |X|$. So we have $|X| \leq |F|$ by above and hence by the Schroeder-Bernstein Theorem (Theorem 0.8.6), $|F| = |X|$. So the result holds for any infinite basis as well. □

Proposition II.1.3

Proposition II.1.3. Let F_1 be the free abelian group on the set X_1 and F_2 the free abelian group on the set X_2. Then $F_1 \cong F_2$ if and only if F_1 and F_2 have the same rank (that is, $|X_1| = |X_2|$).

Proof. Suppose $F_1 \cong F_2$ and let $\alpha : F_1 \to F_2$ be the isomorphism. Since F_1 is a free abelian group on X_1, then X_1 is a basis of F_1 as seen in the proof of Theorem II.1.1. So $\alpha(X_1)$ is a basis of F_2 and $|X_1| = |\alpha(X_1)| = |X_2|$ by Theorem II.1.2.

Suppose F_1 and F_2 have the same rank. Then $|X_1| = |X_2|$ and by Theorem I.7.8, F_1 and F_2 are equivalent. Since the category is the category of abelian groups, then the equivalence is group isomorphism and so $F_1 \cong F_2$. □

Theorem II.1.4

Theorem II.1.4. Every abelian group G is the homomorphic image of a free abelian group of rank $|X|$, where X is a set of generators of G.

Proof. Let F be the free abelian group on the set X. Then $F = \sum_{x\in X} \mathbb{Z}x$ and the rank of F is $|X|$ (see Note 2.1.B). By Theorem II.1.1.(iv) the inclusion map $\iota : X \to G$ induces a homomorphism $\overline{f} : F \to G$ such that $\overline{f}\iota = f$ where $f : x \mapsto 1x$ (since $f : X \to G$ can be any function). So $\overline{f} : 1x \mapsto x$. Whence $X \subseteq \text{Im}(\overline{f})$. Since $\overline{f} : F \to G$ and X generates G, we must have $\text{Im}(\overline{f}) = G$ and G is the image of free group F under homomorphism $\overline{f}$. □

Lemma II.1.5

Lemma II.1.5. If $\{x_1, x_2, \ldots, x_n\}$ is a basis of a free abelian group F and $a \in \mathbb{Z}$, then for all $i \neq j$, $\{x_1, x_2, \ldots, x_{j-1}, x_j + ax_i, x_{j+1}, x_{j+2}, \ldots, x_n\}$ is also a basis of F.

Proof. Since $x_j = -ax_i + (x_j + ax_i)$, it follows that $F = \langle x_1, x_2, \ldots, x_{j-1}, x_j + ax_i, x_{j+1}, \ldots, x_n\rangle$. If

$$k_1x_1 + k_2x_2 + \cdots + k_j(x_j + ax_i) + \cdots + k_nx_n = 0$$

(where $k_i \in \mathbb{Z}$) then

$$k_1x_1 + k_2x_2 + \cdots + (k_i + k_ja)x_i + \cdots + k_jx_j + \cdots + k_nx_n = 0$$

and so each coefficient and hence each k_t equals 0 for all t. So the set is also a basis, as claimed. □

Theorem II.1.6

Theorem II.1.6. If F is a free abelian group of finite rank n and G is a nonzero subgroup of F, then there exists a basis $\{x_1, x_2, \ldots, x_n\}$ of F, an integer r (where $1 \leq r \leq n$) and positive integers $d_1, d_2, \ldots, d_r$ such that $d_1 \mid d_2 \mid \cdots \mid d_r$ (that is, $d_1 \mid d_2$, $d_2 \mid d_3$, $\ldots$, $d_{r-1} \mid d_r$) and G is free abelian with basis $\{d_1x_1, d_2x_2, \ldots, d_rx_r\}$.

Proof. If $n = 1$, then $F = \langle x_1 \rangle \cong \mathbb{Z}$ and $G = \langle d_1x_1 \rangle \cong \mathbb{Z}$ by Theorems I.3.5, I.3.1, and I.3.2. We apply induction and assume the theorem is true for all free abelian groups of rank less than n. Let S be the set of all those integers s such that there exists a basis $\{y_1, y_2, \ldots, y_n\}$ of F and an element in G of the form $sy_1 + k_2y_2 + \cdots + k_ny_n$ (where $k_i \in \mathbb{Z}$). Now $\{y_2, y_1, \ldots, y_n\}$ is also a basis of F and so G has an element of the form $k_2y_2 + sy_1 + \cdots k_ny_n$; hence $k_2 \in S$. Similarly $k_3, k_4, \ldots, k_n \in S$ (by treating each in turn as the "first" element of the finite basis). We have $\{k_2, k_3, \ldots, k_n\} \subset S$. Since $G \neq \{0\}$ by hypothesis, we have $S \neq \varnothing$ (since $\{y_1, y_2, \ldots, y_n\}$ is a basis and $S < G$).

Theorem II.1.6 (continued 1)

Proof (continued). So S contains a least positive integer d_1 and for some basis $\{y_1, y_2, \ldots, y_n\}$ of F there exists $v \in G$ such that $v = d_1y_1 + k_2y_2 + \cdots | k_ny_n$ (by the definition of set S). By the Division Algorithm (Theorem 0.6.3), for each $i = 1, 2, \ldots, n$ we have $k_i = d_1q_i + r_i$ with $0 \leq r_i < d_1$. So

$$v = d_1(y_1 + q_2y_2 + \cdots + q_ny_n) + (r_2y_2 + r_3y_3 + \cdots + r_ny_n).$$

Let $x_1 = y_1 + q_2y_2 + \cdots + q_ny_n$. Then by Lemma II.1.5 (and induction), $W = \{x_1, y_2, \ldots, y_n\}$ is a basis for F. Now by the choice of d_1 (as the smallest coefficient of the first basis element that gives an element of G; since bases can be rearranged, d_1 is the smallest coefficient of *any* basis element that gives an element of G). Since $v \in G$ (with v given above in terms of the y_i's, q_i's, and r_i's) and each $r_i < d_1$ then we have that $0 = r_2 = r_3 + \cdots = r_n$ (or else v is written in terms of $x_1, y_2, \ldots, y_n$ with the coefficients of $y_2, y_3, \ldots, y_n$ are less than d_1, a contradiction). Therefore $d_1x_2 = v \in G$.

Theorem II.1.6 (continued 2)

Proof (continued). Let $H = \langle y_2, y_3, \ldots, y_n \rangle$. Then H is a free abelian group of rank $n - 1$ (since $y_2, y_3, \ldots, y_n$ are "linearly independent" because $\{x_1, y_2, \ldots, y_n\}$ is a basis for F) such that $F = \langle x \rangle \oplus H$. Since $\{x_1, y_2, \ldots, y_n\}$ is a basis of F then $x_1 \notin \langle y_2, y_3, \ldots, y_n \rangle = H$, so $d_1x_1 \notin H$ and $\langle v \rangle = \langle d_1x \rangle \cap H = \{0\}$, which implies $\langle v \rangle \cap (G \cap H) = \{0\}$. If $u = t_1x_1 + t_2x_2 + \cdots + t_ny_n \in G$ (where $t_i \in \mathbb{Z}$) then by the Division Algorithm (Theorem 0.6.3) $t_1 = d_1q_1 + r_1$ where $0 \leq r_1 < d_1$. Thus G contains $u - q_1v = r_1x_1 + t_2y_2 + \cdots + t_ny_n$. The minimality of d_1 in S implies that $r_0 = 0$, whence $t_2y_2 + t_3y_3 + \cdots + t_ny_n \in G \cap H$ and $u = q_1v + (t_2y_2 + t_3y_3 + \cdots + t_ny_n)$. Since u was an arbitrary element of G, then

$$\begin{aligned} G &= \langle v \rangle \oplus (G \cap H) \text{ see Definition I.8.8} \\ &= \langle d_1x_1 \rangle \oplus (G \cap H). \end{aligned}$$

Either $G \cap H = \{0\}$ in which case $G = \langle d_1x_1 \rangle$ and the theorem is true (and $n = 1$), or $G \cap H \neq \{0\}$.

Theorem II.1.6 (continued 3)

Proof (continued). Then by the induction hypothesis (that the result holds for all free abelian groups of rank less than n), there is a basis $\{x_1, x_2, \ldots, x_n\}$ of H and positive integers $r, d_2, d_3, \ldots, d_r$ such that $d_2 \mid d_3 \mid \cdots \mid d_r$ and $G \cap H$ is free abelian with basis $\{d_2x_2, d_2x_3, \ldots, d_rx_r\}$ (here F and G in the statement of the theorem are replaced with H and $G \cap H$, respectively). Since $F = \langle x_1 \rangle \oplus H$ and $G = \langle d_1x_1 \rangle \oplus (G \cap H)$ by the previous paragraph, it follows that $\{x_1, x_2, \ldots, x_n\}$ is a basis of F (since $\{x_2, x_3, \ldots, x_n\}$ is a basis of H by the induction hypothesis) and $\{d_1x_1, d_2x_2, \ldots, d_rx_r\}$ is a basis of G. So to complete the induction step we only need to show that $d_1 \mid d_2$. By the minimality of d_1, $d_1 \leq d_2$. By the Division Algorithm, $d_2 = qd_1 + r_0$ with $0 \leq r_0 < d_1$. Since $\{x_2, x_1 + qx_2, x_3, \ldots, x_n\}$ is a basis of F by Lemma II.1.5 and $r_0x_2 + d_1(x_1 + qx_2) = d_1x_2 + d_2x_2 \in G$. Since r_0 is a coefficient of a basis element which gives an element of G and d_1 is a minimal such positive coefficient, then $r_0 = 0$. Hence $d_2 = qd_1$ and $d_1 \mid d_2$, completing the induction step. □

Corollary II.1.7

Corollary II.1.7. If G is a finitely generated abelian group generated by n elements, then every subgroup H of G may be generated by m elements with $m \leq n$.

Proof. By Theorem II.1.4 there is a free abelian group F of rank n and an onto homomorphism ("epimorphism") $\pi : F \to G$. Now $\pi^{-1}(H)$ is a subgroup of F by Exercise I.2.9(a), and is by Theorem II.1.6 (with m of this theorem being r from there) of rank $m \leq n$. The image under π of any basis of $\pi^{-1}(H)$ is a set of at most m elements (π may not be one to one) that generates $\pi(\pi^{-1}(H)) = H$. So H is generated by $\leq n$ elements. □