Basis Theorem for Finitely Generated Abelian Groups

S. Kumaresan
School of Math. and Stat.
University of Hyderabad
Hyderabad 500046
kumaresa@gmail.com

Lemma 1. *Let $a_1, \dots, a_n$, $(n > 1)$, be integers with g.c.d. 1. then there is an $n \times n$ matrix with integer coefficients whose determinant is 1 in which $a_1, \dots, a_n$ appear as the elements of the first row.*

Proof. For $n = 2$, this is standard. We suppose that for $i = 2, \dots, n-1$, $a_i = b_i d$ where d is the g.c.d. of a_i's. Thus b_i's have g.c.d. 1. By induction b_i are the elements of the first row of a square matrix with determinant 1. $(a_n, d) = 1$ implies there exist $s, t \in \mathbb{Z}$ such that $sa_n + td = 1$. Choose $e \in \{\pm 1\}$ properly. Consider the matrix $\begin{pmatrix} b_1 d & \cdots & b_{n-1}d & a_n \\ & & & 0 \\ & * & & \vdots \\ & & & 0 \\ esb_1 & \cdots & esb_{n-1} & t \end{pmatrix}$.
This is a matrix of the required type. □

Lemma 2. *Let $x_1, \dots, x_n$ be generators of an abelian group written additively. Let $a_1, \dots, a_n$ be integers with g.c.d. 1. Then $a_1x_1 + \cdots + a_nx_n$ may be chosen as one of a set of generators for the group.*

Proof. Let A be as in Lemma 1. Then A^{-1}, the adjoint of A (recall that $A^{-1} = (\det A)^{-1} \cdot \operatorname{adj} A$) has integer entries. Let X be the column vectors on the symbols $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. Then the elements of the group corresponding to the rows of the column vector AX are a set of generators for the group. For $X = A^{-1}X$ so that the generators $x_1, \dots, x_n$ can be expressed as integer combination of the new generators. □

Theorem 3 (Basis Theorem)**.** *If G is a finitely generated abelian group, then G is the direct product of cyclic groups.*

Proof. Choose n such that every set of generators has at least n elements. Choose a set of n generators such that one of them, say, x_n has minimal order, say, k. The other $n-1$ elements generates $H \lneq G$. By induction H is the direct product of cyclic groups. We claim that $H \cap \langle x_n \rangle = \{0\}$. For, if not, there exists integers $a_1, \dots, a_{n-1}$ and $a_n < k$ such that $-a_nx_n +$

$a_1x_1+\cdots+a_{n-1}x_{n-1}=0$. If g.c.d. of $(a_1,\ldots,a_n)$ is d, then $x=\frac{a_1}{d}x_1+\cdots+\frac{a_{n-1}}{d}x_{n-1}-\frac{a_n}{d}x_n$ is an element of a set of n generators of G of order a divisor of $d<a_n<k$. □

Lemma 4. *Let G be a finite abelian group. Let H be any subgroup of G. Then there exists a complement K such that $G=H\oplus K$.*

Proof. Let M be a subgroup such that $M\cap H=(0)$ and M is maximal with this property. We claim that $G=H\oplus M$. If not, then there exists an $x\in G\backslash(H+M)$. We may assume that the order $o(x)$ is minimal with this propery and hence is a prime. Observe that the subgroup $M+<x>$ contains M properly and hence $M+<x>\cap H\neq(0)$. Let $y+jx=h$. Note that $j\neq 0$. Now, $jx\in H+M$ But $<jx>=<x>$ and hence $x\in H+M$, a contradiction. □

The structure theorem for FGA groups in invariant factors form is immediate from this and by induction.

Theorem 5. *Let G be a finite abelian group. Then G is a finite direct sum of cyclic groups H_i, $1\leq i\leq r$ such that $|H_{i+1}|$ divides the order of $|H_i|$ for $1\leq i\leq r-1$.*

Proof. We prove this by induction on $|G|=1$. The result is true if $|G|=1$. Assume that the result is true for all natural numbers less than $n>1$. Let G be a finite abelian of order $n>1$. Let $a\in G$ be of maximal order. Let H_1 be the cyclic group generated by a. If $H_1=G$, there is nothing to prove. If not, by the last lemma there exists a subgroup $M\leq G$ such that $GH_1\oplus M$. Since $|M|<|G|=n$, by induction hypothesis, M is the direct sum of cyclic subgroups H_j, $2\leq j\leq r$ where $|H_{j+1}|$ divides $|H_j|$ for $2\leq j<r$. Assume that H_j is the cyclic subgroup generated by a_j, $2\leq j<n$. Since a is of maximal order, it follows that $o(x)$ divides $o(a)$ for any $x\in G$. In particular, if we let $n_j:=o(a_j)$ it follows that $n_r\mid n_{r-1}\mid\cdots\mid n_2\mid n_1:=m$. The proof is complete. □

1. Let G be a finite abelian group. Let p be a prime such that the order of each element of G is of the form p^r. Then $|G|$ is of the form p^n.

   Trivial, if we use Cauchy's theorem. If q is any prime divisor (other than p) of $|G|$, then there exists an element of order q.

   We use induction to see a direct proof. If G is cyclic, then there is nothing to prove. Choose $e\neq a\in G$. Then $\langle a\rangle$ is a proper subgroup of G. The order of the quotient group $G/\langle a\rangle$ is less than $|G|$. The order of each element of $G/\langle a\rangle$ is a power of p. Hence by induction, the order of $G/\langle a\rangle$ is a power of p. Since $|G|=|G/\langle a\rangle|\times|\langle a\rangle|$, the result follows. □

2. Let G be a finite abelian group of order $p_1^{\alpha_1}\cdots p_n^{\alpha_n}$, where p_i's are distinct prime numbers. Let $G(p_i):=\{x\in G: p_i^{\alpha_i}x=0\}$. Then each $G(p_i)$ is a p_i-subgroup of G.

   It is easy to see that this is a subgroup of G. That it is a p_i-group follows from the last item.

3. With the notation as above, we claim that each $x\in G$ can be written as $x=x_1+\cdots+x_n$ where $x_i\in G(p_i)$, $1\leq i\leq n$. Thus, we have $G=G(p_1)+\cdots+G(p_n)$.

Let q_i be defined by $|G| = p_i^{\alpha_i} q_i$. That is, $q_i = p_1^{\alpha_1} \cdots \widehat{p_i^{\alpha_i}} \cdots p_n^{\alpha_n}$. Since p_i's are distinct, the q_i's have 1 as their GCD. Hence there exists m_i such that $1 = m_1 q_1 + \cdots + m_n q_n$. Hence we have

$$x = 1 \cdot x = m_1 q_1 x + \cdots + m_n q_n x = x_1 + \cdots + x_n, \text{ where} x_i = m_i q_i x.$$

Clearly, $p_i^{\alpha_i} x_i = m_i |G| x = 0$ and hence $x_i \in G(p_i)$.

4. The sum in the last item is direct.

   Enough to show that if $x_1 + \cdots + x_n = 0$, with $x_i \in G(p_i)$, then each $x_i = 0$. Let p_i and q_i be as earlier. Since they are relatively prime, there exists $s, t \in \mathbb{Z}$ such that $sp_i^{\alpha_i} + tq_i = 1$. Note that $x_i = -(x_1 + \cdots + \hat{x}_i + \cdots + x_n)$. We have

   $$x_i = 1 \cdots x_i = sp_i x_i + t \sum_{j \neq i} q_i x_j.$$

   Since $x_i \in G(p_i)$, the first summand is zero. The presence of $p_j^{\alpha_j}$ in q_i ensures $q_i x_j = 0$ for $j \neq i$. Hence we conclude that each $x_i = 0$.

5. We have thus proved the following result known as the primary decomposition theorem:

   Theorem 6. *Let G be a finite abelian group of order $p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, where p_i's are distinct prime numbers. Let $G(p) := \{x \in G : p^\alpha x = 0\}$ where p is one of the p_i's and α is the corresponding α_i.* □

6. Let G be a finite abelian p-group. Let $a \in G$ be of maximal order. Let $H := \langle a \rangle$. Then there exists a subgroup $K \leq G$ such that $G = H \oplus K$.

   To look at the nontrivial part, assume that G is not cyclic. Let $a \in G$ be of maximal order, say, p^m. We claim that there exists an element $x \in G \setminus \langle a \rangle$ of order p.

   Let $b \in G \setminus \langle a \rangle$ be of least possible order. Note that $b \neq 0$. if $pb = 0$, we are through. Assume that $\operatorname{ord} b = p^r$. Consider pb. Its order is p^{r-1}. By our hypothesis on b, pb must be in $\langle a \rangle$. Thus, $pb = ka$. Hence we obtain

   $$0 = p^r b = p^{r1}(pb) = p^{r-1}(ka) = (p^{r-1}k) = a.$$

   Since $\operatorname{ord} a = p^r$, it follows that p^r divides $p^{r-1}k$ and hence p divides k. Therefore, $k = pq$ for some $q \in \mathbb{Z}$. Let $c := b - qa$. Then $c \notin \langle a \rangle$ since otherwise $b = c + qa \in \langle a \rangle$, a contradiction. Also, we have

   $$pc = pb - pqa = pb - ka = 0.$$

   We conclude that $c \notin \langle a \rangle$ is of order p.

   Changing the notation, we may assume that b is of order p. Clearly, $\langle a \rangle \cap \langle b \rangle = (0)$. (For, otherwise $\langle b \rangle \subset \langle a \rangle$.) It follows that the element $a + \langle b \rangle$ is order p^m in the quotient group $G/\langle b \rangle$. By induction hypothesis, there exists a subgroup, say, $\overline{K}$ such that $G/\langle b \rangle = \langle a + \langle b \rangle \rangle \oplus \overline{K}$. Let $K \leq G$ be such that $\overline{K} = K/\langle b \rangle$.

   We claim that $G = K + H$. For, $\langle b \rangle \subset K$, we have $G = K + (\langle a \rangle + \langle b \rangle) = K + \langle a \rangle$.

   We claim that $K \cap \langle a \rangle = (0)$. If $x \in K \cap \langle a \rangle$, then $x \in K \cap (\langle a \rangle + \langle b \rangle) = \langle b \rangle$. Thus $x \in \langle a \rangle \cap \langle b \rangle = (0)$. □

7. Any finite abelian p-group is a direct sum of cyclic p-subgroups.

   Follows by induction and the last result.

8. Are the p-subgroups in the primary decomposition unique?