FINITELY-GENERATED ABELIAN GROUPS

Structure Theorem for Finitely-Generated Abelian Groups. *Let G be a finitely-generated abelian group. Then there exist*

- *a nonnegative integer t and (if $t > 0$) integers $1 < d_1 \mid d_2 \mid \cdots \mid d_t$,*
- *a nonnegative integer r*

such that G takes the form

$$G \approx \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_t\mathbb{Z} \oplus \mathbb{Z}^{\oplus r}.$$

The integers $d_1, \ldots, d_t$ are called the **elementary divisors** *of G. The nonnegative integer r is called the* **rank** *of G. The elementary divisors and the rank of G are unique. The case $t = r = 0$ is understood to mean that G is trivial.*

The argument to be given here is chosen for its resemblance to techniques that one sees in a linear algebra course and for its visual layout. However, the reader should be aware that the argument takes for granted at the outset that the finitely-generated abelian group G has a *presentation*, meaning a description in terms of its generators and relations among them. We will return later in the semester to the fact that a presentation exists.

Proof. The group G is described by a set of r nontrivial integer-linear relations on a minimal set of g generators,

$$\left\{\begin{matrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1g}x_g = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2g}x_g = 0 \\ \vdots \qquad\qquad\qquad\qquad \vdots \\ a_{r1}x_1 + a_{r2}x_2 + \cdots + a_{rg}x_g = 0 \end{matrix}\right\}.$$

Here we assume that $g > 0$, otherwise G is trivial and the result is clear. Also we assume that $r > 0$ since if there are no relations then $G \approx \mathbb{Z}^{\oplus g}$ and we are done. The circumstance that in practice one does not initially know whether a set of generators is minimal will be addressed later in the handout. The relations rewrite more concisely as

$$\sum_{j=1}^{g} a_{ij}x_j = 0, \quad i = 1, \ldots, r.$$

Even more concisely, they encode as an $r \times g$ integer matrix,

$$A = [a_{ij}]_{r \times g}.$$

However, the matrix is not uniquely determined by the group. The following operations on the relations preserve the group that the data describe.

- *Relation recombine.* Replace the ith relation by itself plus k times the jth relation. Here $i, j \in \{1, \ldots, r\}$ with $j \neq i$, and $k \in \mathbb{Z}$. In symbols, $r_i \leftarrow r_i + kr_j$.
- *Relation scale.* Negate the ith relation. Here $i \in \{1, \ldots, r\}$. In symbols, $r_i \leftarrow -r_i$.

- *Relation transposition.* Exchange the ith and the jth relations. Here again $i, j \in \{1, \ldots, r\}$ with $j \neq i$. In symbols, $r_i \leftrightarrow r_j$.

Also, the following operations on the generators preserve the group that the data describe.

- *Generator recombine.* Replace the jth generator by itself minus k times the ith generator. Here $i, j \in \{1, \ldots, g\}$ with $i \neq j$, and $k \in \mathbb{Z}$. In symbols, $x_j \leftarrow x_j - kx_i$. This operation is described slightly differently from the relation recombine above in that i and j have exchanged roles and k is negated; the reason for modifying the description will explain itself in a common description of the two recombines, to arise in a moment.
- *Generator scale.* Negate the ith generator. Here $i \in \{1, \ldots, g\}$. In symbols, $x_i \leftarrow -x_i$.
- *Generator transposition.* Exchange the ith and the jth generators. Here again $i, j \in \{1, \ldots, g\}$ with $j \neq i$. In symbols, $x_i \leftrightarrow x_j$.

The various operations on the data for G translate into row operations and column operations on the describing matrix A for G as follows, letting r stand for *row* and c for *column*.

- *Recombine.* $r_i \leftarrow r_i + kr_j$ or $c_i \leftarrow c_i + kc_j$.
- *Scale.* $r_i \leftarrow -r_i$ or $c_i \leftarrow -c_i$.
- *Transposition.* $r_i \leftrightarrow r_j$ or $c_i \leftrightarrow c_j$.

The recombine operation here is the common description of the two recombine operations above. The operations here are similar to the recombine, scale, and transposition operations that arise in solving a system of linear equations, but the analogy is imperfect. In our context, the matrix A represents the data describing a finitely-generated abelian group, and its entries are integers. Here we are allowed row operations and column operations, but we may scale only by -1. Of course, we may scale vacuously by 1 as well. The real point is that we may scale rows or columns by any invertible integer, i.e., by ± 1; whereas in linear algebra we could scale rows by any invertible field element, i.e., by any nonzero field element.

A small calculation shows that the operations in the previous paragraph have no effect on the greatest common divisor of the matrix entries, $\gcd(\{a_{ij}\})$.

Now to establish the structure of a given finitely-generated abelian group with describing matrix A, proceed as follows. Carry out row and column operation to make the upper left entry of A as small as possible a positive integer d_1 that can be placed there in finitely many steps,

$$A \leftarrow \begin{bmatrix} d_1 & a_{12} & \cdots & a_{1g} \\ a_{21} & a_{22} & \cdots & a_{2g} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \cdots & a_{rg} \end{bmatrix}.$$

Here the entries a_{ij} need not be the original a_{ij}. The a_{ij} will continue to vary throughout the calculation as it proceeds. In fact $d_1 \mid a_{1j}$ for $j = 2, \ldots, g$, else we could make a smaller positive upper left entry, and so after further column operations we may take $a_{1j} = 0$ for $j = 2, \ldots, g$. Similarly we may take $a_{i1} = 0$ for $i = 2, \ldots, r$. And now the same ideas show that $d_1 \mid a_{ij}$ for $i = 2, \ldots, g$ and

$j = 2, \dots, r$. That is, in fact

$$A \leftarrow \left[\begin{array}{c|ccc} d_1 & 0 & \cdots & 0 \\ \hline 0 & a_{22} & \cdots & a_{2g} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{r2} & \cdots & a_{rg} \end{array}\right], \quad 1 \le d_1 \mid a_{ij} \text{ for all } i, j.$$

Because our procedure has had no effect on the greatest common divisor of the matrix entries, we see that in fact d_1 is the greatest common divisor of the original matrix entries.

Our assumption of a minimal set of generators ensures that $d_1 > 1$, strengthening the condition $d_1 \ge 1$ in the previous display, because otherwise the first relation would be $g_1 = 0$, making the generator g_1 superfluous. In practice, one runs the algorithm starting from a set of generators *not* known to be minimal. In that case, if the $d_1 = 1$ scenario arises, i.e., if the original matrix entries have greatest common divisor 1, then rearranging the generators produces a trivial generator that can be ignored, and so the algorithm simply throws out the top row and the left column of A, reindexes, and continues.

Repeating the process until it terminates, we eventually get

$$A \leftarrow \left[\begin{array}{cccc|ccc} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & d_t & 0 & \cdots & 0 \\ \hline 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right], \quad 1 < d_1 \mid d_2 \mid \cdots \mid d_t,$$

and eliminating zero-rows, which encode the trivial relation $0 = 0$, gives

$$A \leftarrow \left[\begin{array}{cccc|ccc} d_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & d_t & 0 & \cdots & 0 \end{array}\right], \quad 1 < d_1 \mid d_2 \mid \cdots \mid d_t.$$

Thus, the group is described by generators $y_1 \dots, y_g$, the first t of them subject to the relations

$$d_1 y_1 = 0, \qquad d_2 y_2 = 0, \qquad \dots, \qquad d_t y_t = 0,$$

and the remaining $r = g - t$ generators free of relations. In other words, any element of G takes the form

$$z = c_1 y_1 + \cdots + c_t y_t + c_{t+1} y_{t+1} + \cdots + c_{t+r} y_{t+r}$$

where

$$0 \le c_1 < d_1, \quad \dots, \quad 0 \le c_t < d_t, \quad c_{t+j} \in \mathbb{Z} \text{ for } j = 1, \dots, r.$$

And thus as claimed,

$$\boxed{G \approx \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_t\mathbb{Z} \oplus \mathbb{Z}^{\oplus r}.}$$

For uniqueness, begin by recalling that the group $\mathbb{Z}$ acts on any abelian group G,

$$\mathbb{Z} \times G \longrightarrow G, \quad (n, g) \longmapsto ng,$$

where the action is by *scaling*,

$$ng = \begin{cases} 0_G & \text{if } n = 0 \text{ (base case),} \\ (n-1)g + g & \text{if } n > 0 \text{ (inductively),} \\ -((-n)g) & \text{if } n < 0 \text{ (reducing to the positive case).} \end{cases}$$

In the third formula, the outer minus sign denotes additive inverse in G while the inner minus sign denotes additive inverse in $\mathbb{Z}$. The fact that scaling gives an action means that

$$(m+n)g = mg + ng, \quad m, n \in \mathbb{Z},\ g \in G,$$

and one should confirm this formula once in one's life; there are cases.

With the action of $\mathbb{Z}$ on G clear, define the *torsion subgroup* of G,

$$G_{\text{tor}} = \{g \in G : ng = 0 \text{ for some } n \in \mathbb{Z}_{>0}\}.$$

The torsion subgroup is intrinsic to G, i.e., its definition makes no reference to the d_i or to r, or even to the presentation of G. Consequently, the *free quotient* of G by its torsion subgroup,

$$G_{\text{free}} = G/G_{\text{tor}}$$

is also intrinsic to G.

The description of G in the box above shows that

$$G_{\text{tor}} \approx \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_t\mathbb{Z},$$

and so there is a resulting second isomorphism

$$G_{\text{free}} \approx \mathbb{Z}^{\oplus r}.$$

It follows that

$$G_{\text{free}}/2G_{\text{free}} \approx (\mathbb{Z}/2\mathbb{Z})^{\oplus r}$$

and thus that

$$|G_{\text{free}}/2G_{\text{free}}| = 2^r.$$

Since $|G_{\text{free}}/2G_{\text{free}}|$ is intrinsic to G, so is r. We note that attempting to argue that the rank must be unique because

> *otherwise an abelian group isomorphism* $\mathbb{Z}^{\oplus r} \approx \mathbb{Z}^{\oplus s}$ *with* $r \neq s$ *would arise, but this is obviously impossible*

misses the point. Such an argument merely begs the question.[1]

Each elementary divisor d_i has a prime factorization,

$$d_i = \prod_p p^{e_{i,p}},$$

and each summand of the torsion group G_{tor} decomposes correspondingly by the Sun-Ze Theorem,

$$\mathbb{Z}/d_i\mathbb{Z} \approx \prod_p \mathbb{Z}/p^{e_{i,p}}\mathbb{Z}.$$

---

[1] *Beg the question* does **not** mean *beg for the question*. Instead, it means to argue circularly that a statement holds because an unsupported rephrasing of the statement holds; or more generally it means to draw the conclusion from an unsupported premise. Misuse of *beg the question* is called *BTQ-abuse*.

Thus as a whole, the torsion subgroup takes the form of a product of prime-power cyclic groups,

$$G_{\text{tor}} \approx \prod_{p,i} \mathbb{Z}/p^{e_{i,p}}\mathbb{Z}.$$

Conversely, given finitely many prime powers, arrange them in a table of right justified rows of the increasing powers of each prime, such as (illustrating by example)

$$\begin{array}{rrrrr} & & 2^5 & 2^{14} & 2^{71} \\ & 3^3 & 3^4 & 3^{200} & 3^{201} \\ & & & & 5^3 \\ 7^2 & 7^4 & 7^{12} & 7^{25} & 7^{90} \\ & 11 & 11^2 & 11^{11} & 11^{121}, \end{array}$$

and form a set of elementary divisors by multiplying the columns,

$$\begin{aligned} d_1 &= 7^2, \\ d_2 &= 3^3 7^4 11, \\ d_3 &= 2^5 3^4 7^{12} 11^2, \\ d_4 &= 2^{14} 3^{200} 7^{25} 11^{11}, \\ d_5 &= 2^{71} 3^{201} 5^3 7^{90} 11^{121}. \end{aligned}$$

Then $d_1 \mid \cdots \mid d_5$ and

$$\prod_{p,i} \mathbb{Z}/p^{e_{i,p}}\mathbb{Z} \approx \prod_i \mathbb{Z}/d_i\mathbb{Z}.$$

Thus, to prove uniqueness of the invariants the issue is to show that if

$$\mathbb{Z}/p^{e_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{e_n}\mathbb{Z} \approx \mathbb{Z}/q^{f_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/q^{f_m}\mathbb{Z}$$

where p, q are prime and $n, m \in \mathbb{Z}_{>0}$ and $1 \le e_1 \le \cdots \le e_n$ and $1 \le f_1 \le \cdots \le f_m$, then $q = p$ and $m = n$ and $f_i = e_i$ for $i = 1, \ldots, n$. We know that the isomorphic groups have the same order,

$$p^{e_1 + \cdots + e_n} = q^{f_1 + \cdots + f_m}.$$

Immediately, $q = p$. The group on the left side has elements of order p^{e_n}, and this is the largest order that any of its elements can have. Similarly for the group on the right side, but with p^{f_m}. Thus $f_m = e_n$, and continuing in a similar fashion completes the argument.

Exercise: For any positive integer n, consider an n-by-n matrix described by Pascal's triangle, exemplified by

$$A_5 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 6 & 10 & 15 \\ 1 & 4 & 10 & 20 & 35 \\ 1 & 5 & 15 & 35 & 70 \end{bmatrix}.$$

What finitely-generated abelian group G_n is described by A_n?

Exercise: Let $(k, +, \cdot)$ be any field, and let $(k^\times, \cdot)$ be its multiplicative group. As a set, $k^\times$ is all of k except 0, but also we are throwing away the addition operation. Let G be any finite subgroup of $k^\times$, possibly $k^\times$ itself if k is finite. Show that G is cyclic. Because the structure theorem is written additively but G is multiplicative, this exercise requires some translation-work.