Abstract Algebra, Lecture 7

The classification of finite abelian groups

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Linköping, fall 2019

Lecture notes availabe at course homepage

http://courses.mai.liu.se/GU/TATA55/

Summary

Summary

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Summary

Summary

1. **Direct products again**
   - Direct sums vs direct products
2. **Torsion and p-groups**
3. **The classification**
4. **Finitely generated (and presented) abelian groups**

For this lecture, all groups will be assumed to be abelian, but will usually be written multiplicatively.

Definition

$G_1, \ldots, G_r$ groups. Their direct product is

$$G_1 \times G_2 \times \cdots \times G_r = \{ (g_1, \ldots, g_r) | g_i \in G_i \}$$

with component-wise multiplication.

Lemma

Put $H_i = \{ (g_1, \ldots, g_r) | g_j = 1$ unless $j = i \}$. Then

1. $H_i \simeq G_i$,
2. $H_1 H_2 \cdots H_r = G$,
3. $H_i \cap H_j = \{1\}$ if $i \neq j$.

Definition

Let G be a group, and $H_1, \ldots, H_K \leq G$. Then G is the internal direct product of $H_1, \ldots, H_k$ if $G \simeq H_1 \times \cdots \times H_k$.

Theorem

TFAE:

1. *G is the internal direct product of $H_1, \ldots, H_k$,*
2. *Every $g \in G$ can be uniquely written as $g = h_1 h_2 \cdots h_k$ with $h_i \in H_i$,*
3. *$H_1 H_2 \cdots H_k = G$ and $H_i \cap H_j = \{1\}$ for $i \neq j$.*

Example

Let $G = C_6 = \langle g \rangle$, $H_1 = \langle g^2 \rangle$, $H_2 = \langle g^3 \rangle$. Then

$$H_1 H_2 = \left\{1, g^2, g^4\right\} \left\{1, g^3\right\} = \left\{1, g^3, g^2, g^5, g^4, g^7 = g^1\right\}$$

and

$$H_1 \cap H_2 = \{1\},$$

so G is the internal direct product of H_1 and H_2. We have that $H_1 \simeq C_3$, $H_2 \simeq C_2$, so $C_6 \simeq C_3 \times C_2$.

Theorem

$C_m \times C_n \simeq C_{mn}$ *iff* $\gcd(m, n) = 1$

Definition

Let I be an infinite index set.

- If G_i is a group for each $i \in I$, then the direct product

$$\prod_{i \in I} G_i$$

  has the cartesian product of the underlying sets of the G_i as its underlying set, and componentwise multiplication
- The direct sum

$$\bigoplus_{i \in I} G_i$$

  is the subgroup of the direct product consisting of all sequences where all but finitely many entries are the corresponding identities

Lemma

If $H_i \leq G$, $H_i \cap H_j = \{1\}$ for $i \neq j$, and for each $g \in G$ there is a finite subset of $S \subset I$ such that

$$g = \prod_{j \in S} h_j, \qquad h_j \in H_j,$$

then

$$G \simeq \oplus_{i \in I} H_i.$$

Definition

- The torsion subgroup of G is the subset of all elements of G of finite order
- If p is any prime number, then the p-torsion subgroup of G is defined as

$$G[p] = \{\, g \in G \,|\, o(g) = p^a \text{ for some } a \in \mathbb{N} \,\}$$

Of course, any finite group is equal to its torsion subgroup.

Definition

G is a p-group if $G = G[p]$.

Lemma

If G is finite, then G is a p-group iff $|G| = p^a$ for some a.

Proof.

If $|G| = p^a$, then by Lagrange $o(g)|p^a$ for all $g \in G$. But the only divisors of p^a are p^b with $b \leq a$.

Conversely, suppose that all G is finite, of size n, where p, q are two distinct prime factors of n. By Cauchy's thm, which we'll prove later, G contains elements of order p, and elements of order q. It is thus not a p-group. □

Example

The torsion subgroup of the circle group $\mathfrak{T}$ consists of all complex numbers

$$z = \exp(\frac{m}{n} 2\pi i), \qquad m, n \in \mathbb{Z}, n \neq 0, \gcd(m, n) = 1$$

and its p-torsion subgroup are those complex numbers where $n = p$.

Lemma

- *The torsion subgroup of G is a subgroup of G, which contains all p-torsion subgroups as subgroups.*
- *The torsion subgroup of G is the direct sum of the $G[p]$ as p ranges over all primes.*

Proof.

Let $o(g) = n < \infty$, with $n = p_1^{a_1} \cdots p_r^{a_r}$. Let, for $1 \le i \le r$, $m_i = n/p_i^{a_i}$, and write $1 = \sum_{i=1}^r m_i x_i$. Put $h_i = g^{m_i x_i}$. Then

$$h_i^{p_i^{a_i}} = g^{m_i x_i p_i^{a_i}} = g^{n x_i} = (g^n)^{x_i} = 1,$$

and $h_i \in G[p_i]$, since $o(h_i) | p_i^{a_i}$. Furthermore,

$$g = g^1 = g^{m_1 x_1 + \cdots + m_r x_r} = g^{m_1 x_1} \cdots g^{m_r x_r} = h_1 \cdots h_r$$

If $u \in G[p] \cap G[q]$ then $o(u) = p^a = q^b$, forcing $a = b = 0$. Thus $G[p] \cap G[q] = \{1\}$.
The previous lemma now shows that G is the internal direct sum of the $G[p]$'s. □

Example

Let again $C_6 = \langle g \rangle$, with $o(g) = 2 * 3 = n$. Put $m_1 = n/2 = 3$, $m_2 = n/3 = 2$, and write

$$1 = 1 * m_1 + (-1) * m_2 = 1 * 3 + (-1) * 2.$$

Put $h_1 = g^3$, $h_2 = g^{-2}$. Then

$$h_1^{2^1} = g^{3*2} = 1, \qquad h_2^{3^1} = g^{-2*3} = 1,$$

so h_1 has 2-torsion, and h_2 has 3-torsion. (In fact, the 2-torsion subgroup is $\langle h_1 \rangle$, and the the 3-torsion subgroup is $\langle h_2 \rangle$.)

We also see that

$$h_1 h_2 = g^3 g^{-2} = g^1 = g$$

Theorem (Classification of the finite abelian groups)

Let G be an abelian group of size $n = p_1^{a_1} \cdots p_r^{a_r}$.

1. $G \simeq \prod_{j=1}^{r} G[p_j]$.
2. *Each p_j-group $G[p_j]$ is isomorphic to a direct product of cyclic p_j-groups.*
3. *A finite abelian p-group with p^a elements is isomorphic to*

$$C_{p^{b_1}} \times \cdots \times C_{p^{b_s}}, \qquad b_1 \geq b_2 \geq \cdots \geq b_r, \quad a = b_1 + \cdots + b_r$$

   and the b_i's are uniquely determined.

4. *Alternatively,*

$$G \simeq C_{d_1} \times \cdots C_{d_\ell}, \qquad d_1 | d_2 | d_3 \cdots | d_\ell,$$

   also uniquely.

Example

What are the isomorphism classes of abelian groups with $36 = 2^2 * 3^2$ elements? We can list them as

$$C_4 \times C_9,\ C_4 \times C_3 \times \mathbb{C}_3,\ C_2 \times C_2 \times C_9,\ C_2 \times C_2 \times C_3 \times C_3,$$

or as

$$C_{36},\ C_3 \times C_{12},\ C_2 \times C_{18},\ C_6 \times C_6.$$

Recall that

$$C_m \times C_n \simeq C_{mn}$$

when $\gcd(m, n) = 1$.

The part of the classification theorem that we have not proved is

Theorem

Every finite p-group is the internal direct sum of cyclic p-groups.

The main step is to establish that

Lemma

If $|G| = p^a$ and $g \in G$ has maximal order p^b, then there is a "complement" $H \leq G$, such that

$$\langle g \rangle H = G, \quad \langle G \rangle \cap H = \{1\}$$

Proof.

See Judson (but note that the desired subgroup is K in his proof). □

Given the lemma, $G \simeq C_{p^b} \times H$, where H is a p-group with p^{a-b} elements; by induction, it can be written as a direct product of cyclic p-groups.

For the remainder of the lecture, groups are abelian, and written additively.

Definition

$\mathbb{Z}^r = \mathbb{Z} \times \mathbb{Z} \times \cdots \mathbb{Z}$ is a *free abelian group* of rank r, as is any group isomorphic to $\mathbb{Z}^r$.

Theorem

The rank is well-defined, i.e.,

$$\mathbb{Z}^r \simeq \mathbb{Z}^s \quad \iff \quad r = s$$

Example

- Free abelian groups are akin to vector spaces.
- Consider $\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z}$: it has an (ordered) *basis*

$$\underline{\mathrm{e}} = [\mathrm{e}_1, \mathrm{e}_2] = [(1, 0), (0, 1)]$$

  w.r.t. which all group elements can be uniquely expressed as integral linear combinations.
- We have similar results regarding subspaces and dimensions as in linear algebra.

Example (contd.)

- Take for example

$$\mathrm{u} = (1,1) = \underline{\mathrm{e}}\begin{pmatrix}1\\1\end{pmatrix}, \; \mathrm{v} = (1,2) = \underline{\mathrm{e}}\begin{pmatrix}1\\2\end{pmatrix}, \; \mathrm{w} = (1,3) = \underline{\mathrm{e}}\begin{pmatrix}1\\3\end{pmatrix}$$

- Then $\langle \mathrm{u}, \mathrm{v}, \mathrm{w} \rangle = \mathbb{Z}^2$, but the vectors are not linearly independent: indeed

$$\mathrm{w} = \frac{1}{2}\mathrm{u} + \frac{1}{2}\mathrm{v},$$

so

$$\mathrm{u} + \mathrm{v} - 2\mathrm{w} = 0.$$

- This means that $\langle \mathrm{v}, \mathrm{w} \rangle = \mathbb{Z}^2$.
- Furthermore, one can check that there are no non-trivial linear relations between v and w, which hence constitute another basis for $\mathbb{Z}^2$.

Theorem

If $H \le G$ with $G \simeq \mathbb{Z}^r$ then H is free abelian of rank $\le r$.

Proof (sketch).

Let G have basis $x_1, \dots, x_r$. Put $G' = \langle x_1, \dots, x_{r-1} \rangle \simeq \mathbb{Z}^{r-1}$ and $H' = H \cap G'$. By induction, H' is free abelian of rank $\le r - 1$. Using the second isomorphism theorem, written additively, we have

$$\frac{H}{H'} = \frac{H}{H \cap G'} \simeq \frac{H + G'}{G'} \subseteq \frac{G}{G'} \simeq \mathbb{Z}$$

We know that any non-trivial subgroup of $\mathbb{Z}$ is isomorphic to $\mathbb{Z}$, so

$$\frac{H}{H'} = \langle v + H' \rangle \simeq \mathbb{Z}$$

for some $v \in H$. That v, together with the basis for H', makes a basis for H. □

Recall that an (abelian or not) group G is finitely generated if there is a finite generating set such that $G = \langle g_1, \ldots, g_r \rangle$.

Theorem

A finitely generated abelian group G can be written as

$$G \simeq G_T \times \mathbb{Z}^r,$$

where G_T is the torsion subgroup, which will be a finite abelian group, and where the rank r is well defined.

Example

A *Klein bottle*
is a two-dimensional closed surface that can be conveniently embedded into $\mathbb{R}^4$, but not (without self-intersection) into $\mathbb{R}^3$. It can be constructed by gluing together a left-twisted Möbius strip with a right-twisted on along their common edge. It is an "non-orientable" surface; this induces torsion in its first "homology group", which is

$$\mathbb{Z}_2 \times \mathbb{Z}.$$

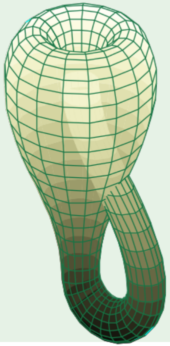
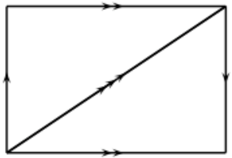


Figure: Klein Bottle

Stolen — from the internet!

But back to the main story. Rather than finding torsion and Betti numbers individually, for simplicial complexes especially, I find it easier to just compute the homology via $H_n = \ker(d_n)/\mathrm{im}(d_{n+1})$. Let's use the following picture:



We have a single 0-simplex, which I'll call v; three 1-simplices, of which the horizontal one will be a, the vertical one b, and the diagonal one c; and two 2-simplices, of which the upper is U and the lower L. I'm orienting the edges in the direction of their arrows; the faces are oriented so that their boundaries are in the direction of two edges, rather than one.

For H_1, you want the 1-cycles mod those that bound a 2-cell. Since each edge is a cycle, the group of 1-cycles is the free abelian group on a, b, c. The boundary of U is $a + b - c$ and that of L is $c + a - b$. So we're looking at $\langle a, b, c\rangle / \langle a + b - c, a - b + c\rangle$. Let's simplify this to $\langle a + b - c, b, c\rangle / \langle a + b - c, 2b - 2c\rangle = \langle b, c\rangle / \langle 2b - 2c\rangle$... and again to $\langle b - c, c\rangle / \langle 2b - 2c\rangle$. Setting $d = b - c$, this is just $\langle d\rangle / \langle 2d\rangle \oplus \langle c\rangle$, which is $\mathbb{Z} \oplus \mathbb{Z}_2$.

Definition

A *finitely presented abelian group* G is given by a finite list of generators $g_1, \ldots, g_n$, and a finite list of relations among the generators, from which all other relations can be derived.

Example

In the Klein bottle example, G is generated by a, b, c, and all relations among the generators are integral linear combinations of

$$a + b - c = 0$$
$$a - b + c = 0$$

For instance, by adding the relations, we conclude that $2a = 0$, so there is 2-torsion in G.

A finitely presented abelian group can be analyzed using the so-called *Smith normal form* of integer matrices:

Example

The relations from the previous example can be summarized as

$$A = \begin{pmatrix} 1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix}$$

By simultaneous (independent) change of bases in the source and in the target, we get

$$D = LAR$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

Example (contd.)

The normal form

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}$$

shows that, in the (first) homology group G of the Klein bottle,

- there is one factor isomorphic to $\mathbb{Z}$,
- there is one factor isomorphic to $\mathbb{Z}_2$,
- the last generator is not needed.