MAT205: Abstract Algebra II

5. Free Abelian Groups and the Subgroup Theorem

Ma, Jia-Jun – Xiamen University Malaysia

Goal of This Lecture

Lay the structural foundation for classifying finitely generated abelian groups.

Target theorem (stacked-basis / subgroup theorem). Let F be a free abelian group of rank n and $K \leq F$ a subgroup. Then there exists a basis $\{x_1, \ldots, x_n\}$ of F and positive integers $d_1 \mid d_2 \mid \cdots \mid d_s$ ($s \leq n$) such that $\{d_1 x_1, \ldots, d_s x_s\}$ is a basis of K.

Roadmap.

1. Understand free abelian groups $\mathbb{Z}^n$ – basis, rank, universal property.
2. Study subgroups $K \leq \mathbb{Z}^n$ – the subgroup theorem.
3. **Next lecture:** uniqueness of d_i, Smith Normal Form, the Fundamental Theorem of F.G. Abelian Groups, applications.

Free Abelian Group: Definition

Definition. An abelian group F is **free abelian** on a set $S \subseteq F$ if every element of F is uniquely expressible as

$$\sum_{s \in S} n_s \cdot s, \qquad n_s \in \mathbb{Z}, \text{ finitely many nonzero}$$

S is called a **basis** for F.

Standard example. $\mathbb{Z}^n = \{(a_1, \ldots, a_n) \mid a_i \in \mathbb{Z}\}$ is free abelian on

$$e_1 = (1, 0, \ldots, 0),\ e_2 = (0, 1, 0, \ldots, 0),\ \ldots,\ e_n = (0, \ldots, 0, 1)$$

Every element has a unique expression $\sum a_i e_i$.

Non-Examples

Definition. $g \in A$ is a **torsion element** if $ng = 0$ for some $n \neq 0$. The **torsion subgroup** is $T(A) = \{g : ng = 0 \text{ for some } n \neq 0\}$. A is **torsion-free** if $T(A) = 0$.

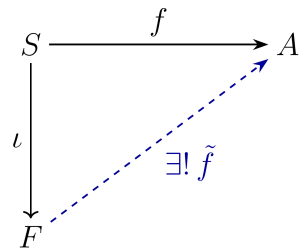
$\mathbb{Z}/n\mathbb{Z}$ is not free abelian: $n \cdot \bar{1} = 0$ – torsion relation on $\bar{1}$.

$\mathbb{Q}$ is torsion-free but still **not free abelian** – it has no basis at all:

- **One element** $a \neq 0$ generates only $a\mathbb{Z}$, missing e.g. $a/2$.
- **Two nonzero elements** $a = p/q,\ b = r/s$ always satisfy $qr \cdot a = pr = ps \cdot b$, so $qr \cdot a - ps \cdot b = 0$ is a nontrivial $\mathbb{Z}$-linear relation.

Universal Property of Free Abelian Groups

Theorem. Let F be free abelian on S. For any abelian group A and any function $f : S \to A$, there is a **unique** group homomorphism $\tilde{f} : F \to A$ extending f.



Concretely: $\tilde{f}\left(\sum n_s s\right) = \sum n_s f(s)$.

Slogan: free abelian groups are defined by **extending any function on the basis linearly**.

This makes F the "most general" abelian group generated by S – no relations except those forced by the abelian axioms.

Rank and the Structure of $\mathbb{Z}^n$

Proposition. F is free abelian with a basis of size $n \iff F \cong \mathbb{Z}^n$.

Proof. $(\Leftarrow)$ $\mathbb{Z}^n$ has basis $\{e_1, \ldots, e_n\}$. ✓

$(\Rightarrow)$ Given basis $S = \{s_1, \ldots, s_n\}$, define $\varphi : \mathbb{Z}^n \to F$ by $\varphi(e_i) = s_i$ (using universal property). Uniqueness of expansion makes φ a bijection. □

Theorem (Rank is well-defined). $\mathbb{Z}^m \cong \mathbb{Z}^n \iff m = n$.

Proof. **Mod out by 2.** For any abelian group A, the quotient $A/2A$ is a well-defined **$\mathbb{F}_2$-vector space** (every element satisfies $2x = 0$). Isomorphic groups give isomorphic quotients, so $|A/2A|$ is an invariant of A.

For $A = \mathbb{Z}^m$: $2A = (2\mathbb{Z})^m$, so $A/2A \cong (\mathbb{Z}/2\mathbb{Z})^m$, a group of order 2^m.

If $\mathbb{Z}^m \cong \mathbb{Z}^n$, then $2^m = |A/2A| = 2^n$, hence $m = n$. □

Definition. The **rank** of a free abelian group is the size of any (hence every) basis.

Subgroups of $\mathbb{Z}$

Warm-up (from Lecture 1): every subgroup of $\mathbb{Z}$ has the form $d\mathbb{Z}$ for some $d \geq 0$.

In particular:

- Every nontrivial subgroup is **isomorphic to** $\mathbb{Z}$ (i.e., free abelian of rank 1)
- The inclusion $d\mathbb{Z} \hookrightarrow \mathbb{Z}$ is given by multiplication by d
- The quotient $\mathbb{Z}/d\mathbb{Z}$ is the **cyclic group** of order d

This is a model for the general picture: subgroups of free abelian groups are themselves free abelian, and the quotients have a clean structure.

Subgroups of $\mathbb{Z}^n$

Theorem. Let $K \leq \mathbb{Z}^n$ be a subgroup. Then:

1. K is **free abelian** of rank $m \leq n$.
2. There exists a basis $v_1, \ldots, v_n$ of $\mathbb{Z}^n$ and positive integers $d_1 \mid d_2 \mid \cdots \mid d_m$ such that $d_1 v_1, \ldots, d_m v_m$ is a basis of K.

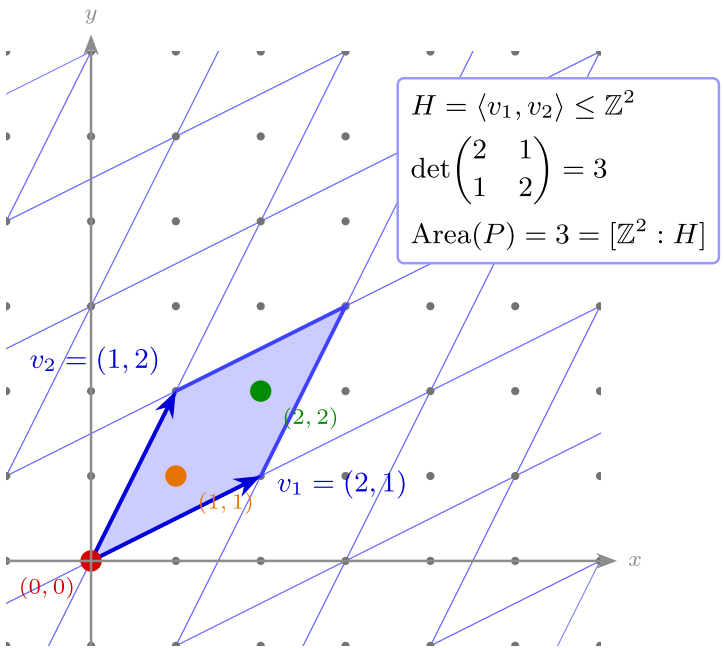
The integers $d_1, \ldots, d_m$ are called the **invariant factors** of K in $\mathbb{Z}^n$, and they are **unique**.

Consequence: the quotient

$$\mathbb{Z}^n / K \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_m\mathbb{Z} \oplus \mathbb{Z}^{n-m}$$

Geometric Picture: Parallelogram Area = Index

$\mathbb{Z}^2$ is a square lattice. A rank-2 sublattice $K = \langle v_1, v_2 \rangle$ is another lattice; its fundamental parallelogram P tiles the plane by translates from K.



Example. $v_1 = (2, 1), v_2 = (1, 2)$:

$$\det \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} = 3.$$

Three cosets of K in $\mathbb{Z}^2$, represented by the integer points of the half-open parallelogram:

$$(0, 0),\ (1, 1),\ (2, 2).$$

General fact. For $K \leq \mathbb{Z}^n$ of full rank with basis $v_1, \ldots, v_n$:

$$[\mathbb{Z}^n : K] \ = \ \left|\det[v_1 \mid \cdots \mid v_n]\right| \ = \ \text{Vol}(P).$$

After Smith Normal Form, $\text{Vol}(P) = d_1 d_2 \cdots d_n$.

Key Lemma: Basis Replacement

Lemma. Let $\{x_1, \dots, x_n\}$ be a basis of a free abelian group F. For any $t \in \mathbb{Z}$ and $i \neq j$, the set

$$\{x_1, \dots, x_{j-1},\ x_j + t x_i,\ x_{j+1}, \dots, x_n\}$$

is again a basis of F.

Proof. **Generates:** $x_j = (-t)x_i + 1 \cdot (x_j + t x_i)$, so the original basis is recoverable. ✓

Linearly independent: suppose

$$n_1 x_1 + \cdots + n_j(x_j + t x_i) + \cdots + n_n x_n = 0.$$

Regrouping gives $n_1 x_1 + \cdots + (n_i + n_j t)x_i + \cdots + n_j x_j + \cdots = 0$. Basis independence of $\{x_i\}$ forces $n_j = 0$ and $n_i + n_j t = 0$, hence $n_i = 0$, and all other $n_k = 0$. □

Slogan. A $\mathbb{Z}$-linear column operation on the basis. The analogue of $C_j \leftarrow C_j + tC_i$ in matrix row-reduction – and, as we'll see next, precisely an **elementary matrix** acting on $B = [x_1 \mid \cdots \mid x_n]$.

Elementary Matrix Viewpoint

Arrange a basis of $F \cong \mathbb{Z}^n$ as the columns of a matrix

$$B \;=\; [\,x_1 \mid x_2 \mid \cdots \mid x_n\,] \;\in\; M_n(\mathbb{Z}).$$

B is a basis $\iff$ B is invertible over $\mathbb{Z}$ $\iff$ $B \in GL_n(\mathbb{Z})$ (i.e. $\det B = \pm 1$).

The basis-replacement lemma in matrix form. Adding t times column i to column j is right-multiplication by the **elementary (transvection) matrix**

$$E_{ij}(t) \;=\; I_n + t\,e_i e_j^{\top} \;=\; \begin{pmatrix} 1 & & & & \\ & \ddots & & t & \\ & & \ddots & & \\ & & & 1 & \\ & & & & \ddots \end{pmatrix} \quad \big(\,t \text{ at entry } (i,j)\,\big).$$

Then $B \cdot E_{ij}(t)$ has the desired new column $x_j + t x_i$, with all other columns unchanged.

Change of Basis $= GL_n(\mathbb{Z})$

Key facts. $\det E_{ij}(t) = 1$, so $E_{ij}(t) \in SL_n(\mathbb{Z})$; and $E_{ij}(t)^{-1} = E_{ij}(-t)$.

Generators of $GL_n(\mathbb{Z})$. Every $U \in GL_n(\mathbb{Z})$ factors as a product of:

Generator	Column operation
Transvection $E_{ij}(t)$	$C_j \leftarrow C_j + t\,C_i$
Permutation P_σ	Swap columns
Sign flip $\mathrm{diag}(\pm 1, \ldots, \pm 1)$	Negate a column

Upshot. Changing basis of $\mathbb{Z}^n \iff$ right-multiplication by some $U \in GL_n(\mathbb{Z})$ – exactly the column operations used in Smith Normal Form.

Subgroup Theorem: Proof Strategy

Goal. Build a basis $\{x_1, \ldots, x_n\}$ of F and positive integers $d_1 \mid \cdots \mid d_s$ so that $\{d_1 x_1, \ldots, d_s x_s\}$ is a basis of K.

Setup. Fix any basis $Y = \{y_1, \ldots, y_n\}$ of F. Every nonzero element of K has a unique expansion

$$k_1 y_1 + k_2 y_2 + \cdots + k_n y_n, \quad \text{some } k_i \neq 0.$$

Key idea (minimality). Over **all** choices of basis Y of F and **all** nonzero elements of K, the set of positive coefficients $|k_i|$ that appear is a nonempty subset of $\mathbb{Z}_{>0}$ – so it has a **minimum** d_1.

Pick a basis Y_1 achieving this minimum, and (after reindexing) pick $w_1 \in K$ with

$$w_1 = d_1 y_1 + k_2 y_2 + \cdots + k_n y_n, \qquad d_1 > 0 \text{ minimal.}$$

Step 1: Producing $d_1 x_1 \in K$

Divide each k_j by d_1: write $k_j = d_1 q_j + r_j$ with $0 \le r_j < d_1$ $(j = 2, \dots, n)$. Then

$$w_1 = d_1 \underbrace{(y_1 + q_2 y_2 + \cdots + q_n y_n)}_{=: x_1} + r_2 y_2 + \cdots + r_n y_n.$$

Claim: $\{x_1, y_2, \dots, y_n\}$ is a basis of F.

Reason. Apply the basis-replacement lemma $n - 1$ times: x_1 was built by adding integer multiples of $y_2, \dots, y_n$ to y_1. ✓

Claim: $r_2 = \cdots = r_n = 0$.

Reason. In the new basis, $w_1 = d_1 x_1 + r_2 y_2 + \cdots + r_n y_n \in K$. If some $r_j > 0$, then $r_j < d_1$ is a strictly smaller nonzero coefficient of an element of K – contradicting the minimality of d_1. □

Conclusion. $d_1 x_1 \in K$, and $\{x_1, y_2, \dots, y_n\}$ is a basis of F.

Step 2: Recursion and $d_1 \mid d_2$

Any $k \in K$ expands as $h_1 x_1 + k_2 y_2 + \cdots + k_n y_n$. Writing $h_1 = d_1 q + r$, minimality of d_1 forces $r = 0$, so $h_1 \in d_1 \mathbb{Z}$. Subtracting $q \cdot (d_1 x_1)$ shows

$$k_2 y_2 + \cdots + k_n y_n \in K.$$

If every such residual is 0, then $K = \langle d_1 x_1 \rangle$ and $s = 1$. Otherwise, **repeat the minimization** on residuals: over bases $\{x_1, y_2, \ldots, y_n\}$, pick the minimum positive $|k_i|$ appearing in a residual. Call it d_2, and (reindexing) obtain $w_2 = d_2 y_2 + k_3 y_3 + \cdots \in K$. As in Step 1, build x_2 with $d_2 x_2 \in K$.

Why $d_1 \mid d_2$. Write $d_2 = d_1 q + r$, $0 \le r < d_1$. The set $\{x_1 + q x_2, x_2, y_3, \ldots, y_n\}$ is a basis (Lemma), and

$$d_1 x_1 + d_2 x_2 \;=\; d_1 (x_1 + q x_2) + r x_2 \;\in\; K.$$

If $r > 0$, then $r < d_1$ is a smaller coefficient – contradicting the minimality of d_1. Hence $r = 0$, i.e. $d_1 \mid d_2$. $\square$

Conclusion of the Proof

Iterate. At step i, we have a basis $\{x_1, \dots, x_i, y_{i+1}, \dots, y_n\}$ of F with $d_1 x_1, \dots, d_i x_i \in K$ and $d_1 \mid d_2 \mid \cdots \mid d_i$. Either every element of K with zero $x_1, \dots, x_i$ components vanishes (stop), or we produce d_{i+1}, x_{i+1} with $d_i \mid d_{i+1}$ as above.

Each iteration **strictly decreases** the rank of the residual lattice, so the process terminates after some $s \leq n$ steps with a basis

$$\{x_1, \dots, x_s, y_{s+1}, \dots, y_n\} \text{ of } F, \qquad \{d_1 x_1, \dots, d_s x_s\} \text{ a basis of } K. \qquad \blacksquare$$

Summary

Concept	Key result
Free abelian group	F with basis S: every element uniquely $\sum n_s s$, $n_s \in \mathbb{Z}$
Universal property	Any $f : S \to A$ extends uniquely to a homomorphism $F \to A$
Rank is well-defined	$\lvert A/2A \rvert$ is intrinsic; for $A = \mathbb{Z}^n$ it equals 2^n
Subgroups of $\mathbb{Z}^n$	Every $K \leq \mathbb{Z}^n$ is free abelian of rank $\leq n$
Stacked basis theorem	Basis $\{x_1, \ldots, x_n\}$ of F with $\{d_1 x_1, \ldots, d_s x_s\}$ a basis of K, $d_1 \mid \cdots \mid d_s$
Proof technique	Minimality of coefficient + division algorithm + basis-replacement lemma
Geometry	$[\mathbb{Z}^n : K] = \lvert\det\rvert = \mathrm{Vol}(P)$ for full-rank K

The setup. The study of subgroups of $\mathbb{Z}^n$ is essentially **linear algebra over $\mathbb{Z}$** – with the crucial subtlety that we can no longer divide.

Looking Ahead

Next (Lecture 6): the classification of finitely generated abelian groups and its applications.

- **Uniqueness** of the invariant factors d_i – they are intrinsic to the quotient F/K.
- **Smith Normal Form** – an algorithm that turns any integer matrix into UDV with $D = \operatorname{diag}(d_1, \ldots, d_r)$ and $d_1 \mid \cdots \mid d_r$.
- **Fundamental Theorem** – every finitely generated abelian group decomposes as $\mathbb{Z}^r \oplus \bigoplus \mathbb{Z}/d_i\mathbb{Z}$.
- **Applications** – $(\mathbb{Z}/n\mathbb{Z})^\times$, finite subgroups of a field, elliptic curves and BSD.

Homework (Lecture 5)

Exercise 1. Show that the torsion set $T(A) = \{a \in A : na = 0 \text{ for some } n \neq 0\}$ is a subgroup of an abelian group A, and that $A/T(A)$ is torsion-free.

Exercise 2. Let M be the $n \times n$ integer matrix whose columns are $x_1, \ldots, x_n \in \mathbb{Z}^n$. Prove that $\{x_1, \ldots, x_n\}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}^n$ iff $\det M = \pm 1$.

Exercise 3. Prove that $\mathbb{Z}^m \ncong \mathbb{Z}^n \oplus T$ whenever $m > n$ and T is a finite abelian group. (Hint: pass to the quotient by torsion; then use the $A/2A$ argument to distinguish $\mathbb{Z}^m$ from $\mathbb{Z}^n$.)

Questions?