Group Theory Lecture Notes (2024/2025)

Griffin Reimerink

Contents

1 Groups

***Definition** Group*

A **group** is a triple $(G, *, e)$ where G is a set, $e \in G$ and $*$ (the **group law**) is a binary map $G \times G \to G$, such that the following three properties hold:

1. **Associativity**: For all $x, y, z \in G$ we have $(x * y) * z = x * (y * z)$
2. **Unit element**: For all $x \in G$, we have $e * x = x = x * e$
3. **Inverses**: For all $x \in G$ a $y \in G$ exists such that $x * y = e = y * x$. (notation: x^{-1})

The order of a group ($\#G$) is its number of elements. We call a group finite if it has finite order.

***Definition** Abelian group*

A group is **abelian** or **commutative** if $g_1 * g_2 = g_2 * g_1 \quad \forall g_1, g_2 \in G$

***Definition** Subgroup*

A group H is a **subgroup** of G if $H \subseteq G$ and they have the same operator and unit element.

***Proposition** Subgroup criterion*

Let $(G, *, e)$ be a group and $H \subseteq G$. Then H forms a subgroup of G if and only if

1. $e \in G$
2. For all $x, y \in H$ also $x * y \in H$
3. For all $x \in H$, also $x^{-1} \in H$

Proposition

The unit element is unique. Inverses are unique.

Proposition

Let G be a group with $g \in G$. Then the maps $x \in G \mapsto g * x$ and $x \in G \mapsto x * g$ are bijective.

***Proposition** Lagrange's theorem*

If H is a subgroup of a finite group G, then the order of H is a divisor of the order of G.

***Definition** Order*

Let x be an element of a group G. We define its **order** (notation: $\text{ord}(x)$) as follows:
If an integer $m > 0$ exists with $x^m = e$, then $\text{ord}(x)$ is defined to be the smallest such m.
Otherwise, we set $\text{ord}(x) := \infty$.

Proposition

Let G be a group and $x \in G$. Then the following statements hold true:

1. $\text{ord}(x) = \text{ord}(x^{-1})$.
2. If $\text{ord}(x) < \infty$, then $\langle x \rangle = \{x, x^2, \ldots, x^{\text{ord}(x)} = e\}$.
3. $\text{ord}(x) = \#\langle x \rangle$, i.e. the order of the subgroup generated by x is the order of x.
4. If $\#G < \infty$, then also $\text{ord}(x) < \infty$ and moreover $\text{ord}(x) \mid \#G$.
5. If $x^n = e$, then $\text{ord}(x) \mid n$

1.1 Homomorphisms

***Definition** Homomorphism*

A **homomorphism** is a map $f : G_1 \to G_2$ such that:

$$f(g_1 * h_1) = f(g_1) * f(h_1) \quad \forall g_1, h_1 \in G_1$$

***Definition** Isomorphism*

An **isomorphism** is a bijective homomorphism.
If an isomorphism between G_1 and G_2 exists, they are **isomorphic**. (notation: $G_1 \cong G_2$)

Proposition *Chinese remainder theorem*

Let N, M be positive integers with $\gcd(N, M) = 1$. The assignment

$$a \bmod NM \mapsto (a \bmod N, a \bmod M) : \mathbb{Z}/NM\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z}$$

is an isomorphism.
Moreover it maps $(\mathbb{Z}/NM\mathbb{Z})^\times$ to $(\mathbb{Z}/N\mathbb{Z})^\times \times (\mathbb{Z}/M\mathbb{Z})^\times$, and this is also an isomorphism.

Proposition *Properties of homomorphisms*

Let $f : G_1 \to G_2$ be a homomorphism and e_1, e_2 the respective units of G_1, G_2. Then,

$$f(g)^{-1} = f(g^{-1}) \qquad f(e_1) = e_2$$

The inverse of an isomorphism is an isomorphism.
The composition of homomorphisms is a homomorphism.

Proposition

Let $f : G_1 \to G_2$ be a homomorphism and H_1, H_2 subgroups of G_1, G_2 respectively.
Then $f(H_1)$ is a subgroup of G_2 and $f^{-1}(H_2)$ is a subgroup of G_1.

Definition *Kernel*

Let $f : G_1 \to G_2$ be a homomorphism. Then $f^{-1}(\{e_2\})$ is the **kernel** of f.

Proposition

Let $f : G_1 \to G_2$ be a group homomorphism.

$$f \text{ is injective} \iff \ker(f) = \{e_1\}$$

2 Permutation groups

Definition *Symmetric group*

For a non-empty set Σ one denotes by S_Σ the set of all bijections from Σ to itself.
The **symmetric group** on the set Σ is defined as the group $(S_\Sigma, \circ, \mathrm{id}_\Sigma)$.

Proposition

Let $f : \Sigma \to \Sigma'$ be a bijection with inverse $g : \Sigma' \to \Sigma$.
Then S_Σ and $S_{\Sigma'}$ are isomorphic, with isomorphism $\varphi : S_\Sigma \to S_{\Sigma'}$ given by $\varphi(\sigma) = f \circ \sigma \circ g$
The inverse of φ is $\psi : S_{\Sigma'} \to S_\Sigma$ given by $\psi(\tau) = g \circ \tau \circ f$.

Proposition *Cayley's theorem*

Every group G is isomorphic to a subgroup of S_G.

Definition *Permutation group*

The symmetric group on n integers, denoted by S_n, is defined as the group $S_{\{1,2,\dots,n\}}$. Elements of this group are called **permutations**. The group S_n is also called the **permutation group** on n elements.

Proposition

Every finite group G is isomorphic to a subgroup of $S_{\{1,\dots,n\}}$.

Proposition

The group S_n consists of $n!$ elements.

2.1 Cycles

Definition *Cycle*

A permutation $\sigma \in S_n$ is called a **cycle** of length k (or a k-cycle), if there exist k distinct integers $a_1, \dots, a_k \in \{1, \dots, n\}$ such that:

$$\sigma(a_i) = a_{i+1} \text{ for } 1 \leq i < k \qquad \sigma(a_k) = a_1 \qquad \sigma(x) = x \text{ for } x \notin \{a_1, \dots, a_k\}$$

Such a permutation is denoted by $\sigma = (a_1\, a_2\, \dots\, a_k)$. A 2-cycle is also called a **transposition**.

Proposition

Any permutation $\sigma \in S_n$ can be written uniquely as a product of pairwise disjoint cycles.

Proposition

If $(a_1 \dots a_k)$ and $(b_1 \dots b_\ell)$ are disjoint cycles, then $(a_1 \dots a_k)(b_1 \dots b_\ell) = (b_1 \dots b_\ell)(a_1 \dots a_k)$

Proposition

Let $\sigma := (i_1\, i_2\, \dots\, i_k)$ be a k-cycle. Then,

$$\sigma^{-1} = (i_k\, i_{k-1}\, \dots\, i_1) \qquad \mathrm{ord}(\sigma) = k$$

Proposition

If $\sigma_1, \dots, \sigma_r$ are pairwise disjoint cycles with lengths ℓ_i, with $\sigma_1 \dots \sigma_r$ denoting their product, then:

- $(\sigma_1 \dots \sigma_r)^n = \sigma_1^n \dots \sigma_r^n$ for all $n \in \mathbb{Z}$
- $\mathrm{ord}(\sigma_1 \dots \sigma_r) = \mathrm{lcm}(\ell_1, \dots, \ell_r)$

Proposition

Every permutation $\sigma \in S_n$ can be written as a product of transpositions.

2.2 Alternating groups

Definition *Sign function*

We define the **sign** of a permutation $\sigma \in S_n$ by

$$\varepsilon(\sigma) := \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} = \pm 1 \;\text{ if } n \geq 2 \qquad \varepsilon(\sigma) := 1 \;\text{ if } n = 1$$

This map is a homomorphism. We call σ **even** if $\varepsilon(\sigma) = 1$ and **odd** if $\varepsilon(\sigma) = -1$.

Proposition

For any $\rho \in S_n$ and any ℓ-cycle $(a_1\, a_2\, \dots\, a_\ell) \in S_n$,

$$\rho(a_1\, a_2\, \dots\, a_\ell)\rho^{-1} = (\rho(a_1)\, \rho(a_2)\, \dots\, \rho(a_\ell))$$

Proposition

Every transposition is odd.

Definition *Alternating group*

For $n \geq 1$ the **alternating group** A_n is the subgroup of S_n consisting of all even permutations.

Proposition

1. An ℓ-cycle has sign $\varepsilon(\sigma) = (-1)^{\ell - 1}$
2. If σ is a product of cycles of lengths $\ell_1, \dots, \ell_r$, then $\varepsilon(\sigma) = (-1)^n$ where $n = \sum_{i=1}^r (\ell_i - 1)$
3. A permutation σ is even if and only if σ can be written as a product of an even number of 2-cycles.

Proposition

For $n \geq 2$ the group A_n consists of $\frac{n!}{2}$ elements.

Proposition

For $n \geq 3$ the elements of A_n can be written as products of 3-cycles.

3 Symmetry groups

Definition *Groups of matrices*

The **general linear group** $GL_n(F)$ is the group of invertible $n \times n$ matrices in the field $F = \mathbb{R}$ or $F = \mathbb{C}$. Its group law is matrix multiplication and the unit element is the identity matrix.

Let $n \in \mathbb{Z}, n > 0$. We define:

- The **orthogonal group** $O(n) := \{A \in GL_n(\mathbb{R}) \mid A^*A = I\}$
- The **unitary group** $U(n) := \{A \in GL_n(\mathbb{C}) \mid A^*A = I\}$
- The **special orthogonal group** $SO(n) := \{A \in GL_n(\mathbb{R}) \mid A^*A = I \text{ and } \det(A) = 1\}$
- The **special unitary group** $SU(n) := \{A \in GL_n(\mathbb{C}) \mid A^*A = I \text{ and } \det(A) = 1\}$

Definition *Isometry*

An **isometry** on $\mathbb{R}^n$ is a map $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ with the following property:

$$\|v - w\| = \|\varphi(v) - \varphi(w)\|$$

The group of all isometries on $\mathbb{R}^n$ is denoted $\mathrm{Isom}(\mathbb{R}^n)$.

Proposition

1. An isometry on $\mathbb{R}^n$ mapping $0 \in \mathbb{R}^n$ to 0 is linear.
2. The linear isometries on $\mathbb{R}^n$ are exactly the elements of $O(n)$.
3. Every isometry can be written as a composition of a translation and a linear isometry.
4. Isometries are invertible.

Definition *Symmetry group*

The **symmetry group** of a subset $F \subset \mathbb{R}^n$ is defined as:

$$\mathrm{Sym}(F) := \{\varphi \in \mathrm{Isom}(\mathbb{R}^n) \mid \varphi(F) = F\}$$

Proposition

Let $F \subset \mathbb{R}^n$, $a \in \mathbb{R}_{>0}$ and φ an isometry on $\mathbb{R}^n$. Then $\mathrm{Sym}(F)$ and $\mathrm{Sym}(a\varphi(F))$ are isomorphic.

3.1 Dihedral groups

Definition *Dihedral group*

The symmetry group of a regular n-gon F_n is called the n-th **dihedral group** D_n.
The symmetry group of the circle C_r is called the **infinite dihedral group** D_∞.

Proposition *Properties of D_∞*

The group D_∞ is isomorphic to $O(2)$, and consists of reflections σ across arbitrary lines through the center of the circle, and of all rotations ρ around the center of the circle.
The subset $R \subset D_\infty$ of all rotations is a commutative subgroup of D_∞.
For any reflection $\sigma \in D_\infty$, we have $D_\infty = R \cup R \cdot \sigma$.

Proposition *Properties of D_n*

The group D_n consists of $2n$ elements. It is abelian if and only if $n = 2$.
The group D_n contains the rotation ρ by an angle $\frac{2\pi}{n}$ and the reflection σ in the x-axis.
Every element of D_n can be written in a unique way as ρk or $\sigma\rho k$, for some $0 \le k < n$.
We have $\rho^n = \sigma^2 = \mathrm{id}$. The subgroup R_n of D_n consisting of all rotations is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

3.2 Automorphisms of graphs

Definition *Automorphism of a graph*

An **automorphism** of a graph $\Gamma = (V, E)$ is a permutation σ on its set of vertices V,
with the property that for all $\{a, b\} \in E$ also $\{\sigma(a), \sigma(b)\} \in E$.
The set consisting of all automorphisms of Γ is denoted $\mathrm{Aut}(\Gamma)$

Proposition

For a graph Γ with n vertices, $\mathrm{Aut}(\Gamma)$ is a subgroup of S_n.

4 Actions and Sylow theory

Definition *Coset, index*

A **left coset** of H in G is any subset of the form $gH, g \in G$.
A **right coset** of H in G is any subset of the form $Hg, g \in G$.
The set of all left cosets $\{gH : g \in G\}$ is denoted G/H. The set $\mathbb{Z}/n\mathbb{Z}$ is an example of this notation.
The **index** $[G : H]$ of H in G is defined as the number of disjoint left cosets $(\#G/H)$ of H in G.

4.1 Conjugation

Definition *Conjugation*

If G is a group and $a \in G$, then the map $\gamma_a : G \to G, x \mapsto axa^{-1}$ is called the **conjugation** by a.
"x and y are **conjugate**" (notation: $x \sim y$) means $y = axa^{-1}$ for some $a \in G$.
The **conjugacy class** of x is $C_x = \{y \in G \mid$ there exists $a \in G$ with $\gamma_a(x) = y\}$.

Proposition *Properties of conjugation*

Let G be a group and $a, b \in G$.

1. Conjugation is an isomorphism.
2. $\gamma_a\gamma_b = \gamma_{ab}$
3. The inverse of γ_a is $\gamma_{a^{-1}}$.
4. If H is a subgroup of G, then $\gamma_a(A) = aHa^{-1}$ and $H \cong aHa^{-1}$
5. $a \sim b$ is an equivalence relation.
6. G is the disjoint union of conjugacy classes.

4.2 Group actions

Definition *Group action*

A **group action** of a group G on a nonempty set X is a map $G \times X \to X$, denoted $(g, x) \mapsto gx$, satisfying:

1. $ex = x$ for every $x \in X$
2. $(gh)x = g(hx)$ for all $g, h \in G$ and all $x \in X$

Alternative terminology: "X is a G-set", "G acts on X"

Proposition

Let G be a group and X a set.

- Given an action of G on X, the map $f : G \to S_X$ given by $f(g)(x) = gx$ is a homomorphism.
- If $f : G \to S_X$ is a homomorphism, then $gx := f(g)(x), g \in G, x \in X$ defines an action of G on X

Definition *Stabilizer and orbit*

Let the group G act on the set X and take $x \in X$.

- The **stabilizer** of x in G, denoted by G_x or by $\mathrm{Stab}_G(x)$, is:

$$G_x := \{g \in G : gx = x\} \subseteq G$$

- The **orbit** of x under G, denoted by Gx, is:

$$Gx := \{gx : g \in G\} \subseteq X$$

Definition *Faithful and transitive actions*

The action of G on X is called **faithful** if for all $g, h \in G$ with $g \neq h$ there exists $y \in X$ with $gy \neq hy$.
The action of G on X is called **transitive** if for all $x_1, x_2 \in X$ there exists $g \in G$ with $gx_1 = x_2$

Definition *Fixpoints*

The element $x \in X$ is called a **fixpoint** or **invariant** of G if $gx = x$ for every $g \in G$.
The **set of fixpoints** of G is denoted as:

$$X^G = \{y \in X : gy = y \text{ for all } g \in G\}$$

The action of G on X is called **fixpoint free** if there are no fixpoints.

Proposition *Properties of group actions*

Let G be a group and let X be a G-set. Let f be the map $G \to S_x$ given by $f(g)(x) = gx$.

1. For any $x \in X$, the stabilizer G_x is a subgroup of G.
2. The action of G on X is faithful $\iff$ The map f is injective
3. G acts transitively on X $\iff$ $Gx = X$ for some $x \in X$ $\iff$ $Gx = X$ for all $x \in X$
4. Let $x, y \in X$. Then $Gx = Gy$ $\iff$ $y \in Gx$, and $Gx \cap Gy = \varnothing$ $\iff$ $y \notin Gx$.
5. Let $x \in X$ and $g \in G$. Then $G_{gx} = gG_xg^{-1}$ (conjugation by g is an isomorphism $G_x \cong G_{gx}$)
6. X is a disjoint union of orbits.

Proposition

Suppose G is a group and X is a G-set. Let $x \in X$.
Then $G/G_x \to Gx : gG_x \mapsto gx$ is a well-defined bijective map.

Proposition

For any G-set X and any $x \in X$ one has $\#Gx = [G : G_x]$

Definition *Permutation character*

Given a group G and a finite G-set X, the **permutation character** of the action is:

$$\chi : G \to \mathbb{Z} \qquad \chi(g) := \#\{x \in X : gx = x\} = \#\text{fixpoints of } g$$

Proposition *Orbit-counting formula*

Let G be a finite group acting on a finite G-set X . The number of orbits in X under G is given by:

$$\#\text{orbits} = \frac{1}{\#G} \sum_{g \in G} \chi(g)$$

4.3 Sylow theory

Definition *Sylow p-group*

Let G be a finite group and let p be a prime dividing the order of G.
Write $\#G = p^n \cdot m$ with $n \geq 1$, $\gcd(p, m) = 1$. A **Sylow p-group** in G is a subgroup of G with order p^n.
We define $n_p(G)$ to be the number of distinct Sylow p-groups in G.

Proposition *Properties of Sylow p-groups*

Let G be a finite group and let p be a prime dividing $\#G$. Consider m, n by definition of Sylow groups.

- The group G contains a Sylow p-group.
- $n_p(G) \equiv 1 \mod p$
- If H_1, H_2 are both Sylow p-groups in G, then they are conjugate. ($H_1 = \gamma_a(H_2)$ for some $a \in G$)
- $n_p(G) \mid m$

Proposition

For p prime and $n, m > 0$ with $\gcd(p, m) = 1$ we have $\binom{p^n m}{p^n} \equiv 1 \mod p$

Proposition

Suppose $p \neq q$ are primes with $p \neq 1 \mod q$ and $q \neq 1 \mod p$, and G is a group with $\#G = pq$. Then $G \cong \mathbb{Z}/pq\mathbb{Z}$, i.e. there is only 1 group with order pq up to isomorphism, which is the cyclic group.

Proposition *Cauchy's theorem*

If G is a finite group and if p is a prime dividing the order of G, then there exists $g \in G$ with $\mathrm{ord}(g) = p$.

5 Normal subgroups and factor groups

5.1 Normal subgroups

Definition *Normal subgroup*

A subgroup H of a group G is called a **normal subgroup** if $H = aHa^{-1}$ for all $a \in G$.

Proposition

If H is a subgroup of a group G and $a, b \in G$, then

$$aH = bH \iff b^{-1}a \in H$$

Proposition

Let G be a group and let $H \subseteq G$ be a subgroup. The following statements are equivalent:

1. H is normal in G
2. $aH = Ha$ for all $a \in G$
3. $aHa^{-1} \subseteq H$ for all $a \in G$
4. For all $a, b, c, d \in G$ with $aH = cH$ and $bH = dH$ we also have $abH = cdH$

Proposition

If G is a group and if H is a subgroup of G with $[G : H] = 2$, then $H \subseteq G$ is normal.

5.2 Factor groups

Definition *Factor group*

Given a group G and a normal subgroup $H \subseteq G$, the **factor group** G modulo H is:

$G/H := \{aH \mid a \in G\}$ Unit element: $eH = H$ Group law: $(aH) \cdot (bH) := abH$

Proposition

Let H be a normal subgroup of a group G.

$$G/H \text{ abelian} \iff a^{-1}b^{-1}ab \in H \quad \text{for all } a, b \in G$$

Proposition

Let H be normal in a group G.
The assignment $\pi : G \to G/H : g \mapsto gH$ defines a surjective homomorphism from G to G/H with $\ker(\pi) = H$.
This is called the **canonical homomorphism** to a factor group.

Proposition

A subgroup H of a group G is normal if and only if H is the kernel of some homomorphism from G to another group.

5.3 Simple groups

Definition *Simple group*

A group G is called **simple** if $\{e\}$ and G are the only normal subgroups in G.

Proposition

A_n is a simple group for every $n \geq 5$.

5.4 Homomorphisms from factor groups

Proposition

Let G, G' be groups, let H be a normal subgroup of G, and $\varphi : G \setminus H \to G'$ a homomorphism.
Consider the canonical homomorphism $\pi : G \to G/H$ given by $\pi(g) = gH$.
Then the composition $\psi = \varphi \circ \pi$ is a homomorphism $G \to G'$, which satisfies $H \subset \ker(\psi)$.

Construction of a homomorphism from a factor group

Let H be a normal subgroup of a group G, and consider an arbitrary group G'.
We can construct a homomorphism $\varphi : G/H \to G'$ as follows:

1. Find a homomorphism $\psi : G \to G'$ satisfying $H \subset \ker(\psi)$
2. We have $\psi(g_1) = \psi(g_2)$ for all $g_1, g_2 \in G$ such that $g_1H = g_2H$,
   i.e. the rule $\varphi(gH) = \psi(g)$ yields a well-defined map $G/H \to G$
3. $\varphi : G/H \to G'$ is a homomorphism, and $\psi = \varphi \circ \pi$ where π is the canonical homomorphism $G \to G/H$.

5.5 Isomorphism theorems

Proposition *Homomorphism theorem*

Let $\psi : G \to G'$ be a homomorphism of groups and $H := \ker(\psi)$. Then:

1. H is a normal subgroup of G
2. $G/H \cong \psi(G)$
3. $\psi(G)$ is a subgroup of G'
4. If ψ is surjective, then $G/H \cong G'$

Proposition *First isomorphism theorem*

Consider a group G, a subgroup $H \subseteq G$, a normal subgroup $N \subseteq G$, and the group $HN = \{hn \mid h \in H, n \in N\}$.

1. HN is a subgroup of G.
2. N is a normal subgroup of HN.
3. $H \cap N$ is a normal subgroup of H
4. $H/(H \cap N) \cong HN/N$

Proposition *Second isomorphism theorem*

Consider a group G and a normal subgroup N.

1. Every normal subgroup in G/N has the form H/N, where H is a normal subgroup in G containing N.
2. If $N \subset H$ for some normal subgroup H in G, then $(G/N)/(H/N) \cong G/H$.

6 Finitely generated abelian groups

Definition *Finitely generated group*

A group G is **finitely generated** if it contains a finite set of **generators** $g_1, g_2, \ldots, g_n$ such that every element of G can be written as a product of the generators and their inverses.
The group law of finitely generated abelian groups will be denoted by $+$.

Proposition

Any finitely generated abelian group $(A, +, 0)$ is isomorphic to a factor group $\mathbb{Z}^n/H$ for some subgroup $H \subseteq \mathbb{Z}^n$

Proposition

If $\mathbb{Z}^k \cong \mathbb{Z}^\ell$, then $k = \ell$.

Proposition

If H is a subgroup of $\mathbb{Z}^n$ then a unique k exists with $H \cong \mathbb{Z}^k$ and $0 \leq k \leq n$.

Definition *Free abelian group*

An abelian group H is called a **free abelian group** if a **basis** $h_1, \ldots, h_k \in H$ exists such that every $h \in H$ can be written uniquely as $h = m_1 h_1 + \ldots + m_k h_k$.

6.1 The structure of finitely generated abelian groups

Proposition *Structure theorem for finitely generated abelian groups*

For any finitely generated abelian group A there exist a unique integer $r \geq 0$ and a unique (possibly empty) finite sequence $(d_1, \ldots, d_m)$ of integers $d_i > 1$ satisfying $d_m \mid d_{m-1} \mid \ldots \mid d_1$ such that

$$A \cong \mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_m\mathbb{Z}$$

We call r the **rank** of A and we call $d_1, \ldots, d_m$ the **elementary divisors** of A.

Proposition

Let H be a subgroup of $\mathbb{Z}^n$ with $H \neq \{0\}$.
There exists a basis $f_1, \ldots, f_n$ for $\mathbb{Z}^n$, and a sequence of integers $(d_1, \ldots, d_k)$ of length $1 \leq k \leq n$ with $d_i > 0$ and $d_k \mid d_{k-1} \mid \ldots \mid d_1$, such that $d_1 f_1, \ldots, d_k f_k$ is a basis for H.

Definition *Torsion subgroup*

Let A be an abelian group. The subgroup $A_{\text{tor}} = \{a \in A \mid \operatorname{ord}(a) < \infty\}$ is called the **torsion subgroup** of A.

Proposition

Suppose that H is a subgroup of $\mathbb{Z}^n$ generated by $g_1, \ldots, g_n$ and $g_i = a_{1i}e_1 + \ldots + a_{ni}e_n$ for some basis $\{e_1, \ldots, e_n\}$ for $\mathbb{Z}^n$. Let $A = (a_{ij})$ be the corresponding $n \times n$ matrix. Then:

$$H \text{ has finite index in } \mathbb{Z}^n \iff \det(A) \neq 0 \implies \#\mathbb{Z}^n/H = |\det(A)|$$

Index