Fields and vector spaces

Žiga Virk

October 20, 2021

The material presented up to this point mostly falls into the premise of geometric topology and combinatorics: we introduced metric spaces and their combinatorial descriptions, simplicial complexes. Our eventual goal however is to compute meaningful topological invariants from these combinatorial descriptions. Within mathematics the field dealing with operations is called algebra and our milestone on the path to computational implementation is an algebraic formulation based on simplicial complexes. With that intention in mind we first review and introduce some algebraic concepts.

In this lecture we will present fields and vector spaces. Specific cases of the first two notions are probably familiar to the reader: real numbers and vectors in Euclidean space. We will introduce a few more fields and vector space constructions, which will provide us with enough structure to introduce homology in the next chapter.

1 Fields

Within the context of algebra, a field is a set with two operations satisfying a number of properties. For our purposes we will deflect a formal introduction and rather introduce specific fields which will be of our interest.

We will think of a field as our number system. We will want to be able to **add, subtract, multiply and divide (except by zero)** in our field. The fields a reader is most familiar[1] with are probably $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$. However, there is also a family of finite fields (consisting of finitely many numbers) which often provides convenient examples: the reminders.

[1] $\mathbb{N}$ is not a field as it does not contain all results of subtractions, for example, $3 - 5 \notin \mathbb{N}$. $\mathbb{Z}$ is is not a field as it does not contain all quotients by non-zero numbers, for example $3/5 \notin \mathbb{Z}$.

The fields of remainders $\mathbb{Z}_p$

Definition 1.1. *Let $p \in 2, 3, 5, \ldots$ be a prime number. Define:*

(a) $p\mathbb{Z} = \{p \cdot n \quad | \, n \in \mathbb{Z}\} = \{\ldots, -2p, -p, 0, p, 2p, 3p, \ldots\}$;

(b) $\mathbb{Z}_p = \mathbb{Z}/(p\mathbb{Z})$ *as the quotient consisting of* ***remainders when dividing by*** p.

Let us discuss *(b)*[2] in detail. The **quotient** $\mathbb{Z}/(p\mathbb{Z})$ consists of classes, each of which can be represented by a number from the "numerator" $\mathbb{Z}$. If $a \in \mathbb{Z}$ then the corresponding class is represented by $[a]$. Two such numbers represent the same class in the quotient iff their difference is[3] in the "denominator" $\mathbb{Z}_p$. To phrase it differently[4],

[2] I.e., the fields of remainders and the quotient construction that defines it.

[3] I.e., iff their difference is a multiple of p. In particular this means $[a] = [b]$ if the remainder after dividing by p is the same for both a and b.

[4] What we just described is a general construction of an algebraic quotient structure. We will come across it again in the context of vector spaces.

$$[a] = [b] \quad \Leftrightarrow \quad b - a \in p\mathbb{Z}.$$

Example 1.2. *Let $p = 5$. In $\mathbb{Z}_5$ two numbers represent the same class iff their difference is divisible by 5. Classes $[0], [1], [2], [3], [4]$ are all distinct but*[5]*:*

- $[5] = [0]$ *as* $5 - 0 = 1 \cdot 5$.
- $[6] = [1]$ *as* $6 - 1 = 1 \cdot 5$.
- $[-1] = [4]$ *as* $-1 - 4 = -1 \cdot 5$.
- $[126] = [1]$ *as* $126 - 1 = 25 \cdot 5$.

In particular, two numbers represent the same class iff their remainder when dividing by 5 is the same.

[5] A few more examples in $\mathbb{Z}_5$: $[-4] = [1], [8] = [3], [17] = [2]$, $[1346134523451] = [1], [3457] = [2]$, $[-23513252] = [3]$.

☞ A few examples in $\mathbb{Z}_7$: $[8] = [1] = [15]$, $[-5] = [2] = [72]$.

We can draw another conclusion from Example 1.2: the most convenient representation[6] of $\mathbb{Z}_p$ is given by p classes $[0], [1], \ldots, [p-1]$. These classes are all distinct[7] and together form $\mathbb{Z}_p$.

[6] We will actually be using this representation almost exclusively from now on.

[7] They form all possible remainders after division by p.

Example 1.3. *The structure of $\mathbb{Z}_2$ encodes parity: for $a \in \mathbb{Z}$ we observe that $[a] = 0$ iff a is even, and $[a] = 1$ iff a is odd.*

Defining the addition, subtraction and multiplication in $\mathbb{Z}_p$ These three operations are defined in the obvious way:

$$[a] + [b] = [a + b], \quad [a] - [b] = [a - b] \quad \text{and} \quad [a] \cdot [b] = [a \cdot b].$$

It turns out that the operations is well defined[8] in the following sense:

$$[a] = [a'], [b] = [b'] \implies [a + b] = [a' + b']$$

and the same holds for the subtraction and multiplication.

[8] Let us prove that addition is well defined.

Proof.

$$[a] = [a'], [b] = [b'] \implies$$

$$\exists k_a, k_b \in \mathbb{Z} : a' = a + k_a p, b' = b + k_b p.$$

Thus

$$[a' + b'] = [a + k_a p + b + k_b p] =$$

$$= [(a + b) + (k_a + k_b)p] = [a + b].$$

□

Example 1.4. *Addition:*
In $\mathbb{Z}_5$: $[3] + [4] = [2], [3] - [4] = [4], [1] + [2] = [3]$.
In $\mathbb{Z}_7$: $[3] + [4] = [0], [3] - [4] = [6], [1] + [2] = [3]$.
Multiplication:
In $\mathbb{Z}_5$: $[3] \cdot [4] = [2], [2] \cdot [4] = [3], [2] \cdot [3] = [1]$.
In $\mathbb{Z}_7$: $[3] \cdot [4] = [5], [2] \cdot [4] = [1], [2] \cdot [3] = [6]$.

Example 1.5. *Note that in $\mathbb{Z}_2 = \{[0], [1]\}$ we have $[a] = [-a]$ hence addition is the same as subtraction. In fact, if we identify $[0]$ and $[1]$ with their Boolean values, the addition and multiplication encode*[9] *logical operations "Exclusive or" (XOR) and "Conjunction" (AND):*

$$[a] + [b] = [a \ XOR \ b], \quad [a] \cdot [b] = [a \ AND \ b].$$

[9] Which means, amongst others, that these operations in $\mathbb{Z}_2$ are fairly natural in computer, exact, and fast. In fact, computations in topological data analysis are often performed using $\mathbb{Z}_2$.

Defining the division in $\mathbb{Z}_p$

Up to this point the described structure of $\mathbb{Z}_p$ did not require[10]

[10] ...as assumed in Definition 1.1.

p to be prime. This assumption however is required[11] if we want to define division by classes, which are different than $[0]$. From the number theory we know that if p is a prime, then for each number $a \in \mathbb{Z}$ with $[a] \neq [0]$, the classes $[a], [2a], \dots [pa] = [0]$ represent the entire $\mathbb{Z}_p$. In particular, we can choose a coefficient k representing $[1] = [kp]$ and define the inverse of p by $[p]^{-1} = [k]$. We can consequently define the division by

$$[a]/[b] = [a] \cdot [b]^{-1},$$

which turns out to be well defined if p is prime and $[b] \neq [0]$.

Example 1.6. *In $\mathbb{Z}_5$ we have $[1 \cdot 3] = [3], [2 \cdot 3] = [1], [3 \cdot 3] = [4], [4 \cdot 3] = [2], [5 \cdot 3] = [0 \cdot 3] = [0]$. The products $[k \cdot 3]$ exhaust entire $\mathbb{Z}_5$ and $[3]^{-1} = [2]$. Similarly, $[2]^{-1} = [3]$.*

In $\mathbb{Z}_7$ we have $[2]^{-1} = [4]$, $[3]^{-1} = [5]$, ...

We are now able to add, subtract, multiply and divide (except by zero) in $\mathbb{Z}_p$, which makes $\mathbb{Z}_p$ a field.

Remark 1.7. *Counting and computing in $\mathbb{Z}_p$ is surprisingly common in everyday life. It appears whenever we have a periodic behaviour.*

- *$\mathbb{Z}_2$ is a model for true/false in logic, odd/even numbers, etc.*
- *We use $\mathbb{Z}_4$ when thinking about seasons of the year.*
- *We use $\mathbb{Z}_7$ when thinking about days of the week (if today is the a^{th} day of the week then b days from today it will be $[a+b]^{th}$ day of the week).*
- *We use $\mathbb{Z}_{10}$ whenever we are computing in decimal numbers. Given $a, b \in \mathbb{N}$, the first digit of $a+b$ equals $[a+b]$ in $\mathbb{Z}_{10}$ and the same goes for multiplication.*
- *We use $\mathbb{Z}_{10}$ whenever we are converting in the metric system*[12].
- *We use $\mathbb{Z}_{24}$ when thinking about hours in a day*[13].
- *We use $\mathbb{Z}_{60}$ when thinking about minutes and seconds.*

As a summary let us recall all the fields we mentioned: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, and $\mathbb{Z}_p$ for any prime number p. These are the only fields we will be considering[14].

2 Vector spaces

A prototype of a vector space over field $\mathbb{R}$ a reader is familiar with is $\mathbb{R}^n$ for any $n \in \mathbb{N}$. It consists of n-tuples (vectors) of real numbers, which we can add, subtract, and multiply by any element of our field $\mathbb{R}$. In a similar way $\mathbb{F}^n$ is a vector field over $\mathbb{F}$: it consists of n-tuples

[11] If q is not a prime then $\mathbb{Z}_q$ contains *divisors of zero*, i.e., non-zero classes, whose product is the zero class. For example, $[2] \in \mathbb{Z}_4$ is a non-zero class, but $[2] \cdot [2] = [4] = [0] \in \mathbb{Z}_4$ is the zero class. If we wanted to find an inverse of $[2]$ in $\mathbb{Z}_4$ we would need to find an integer $k \in \mathbb{Z}$, so that $[2k] = [1] \in \mathbb{Z}_4$, an unattainable feat as $2k$ is always even. A divisor of zero has no inverse.

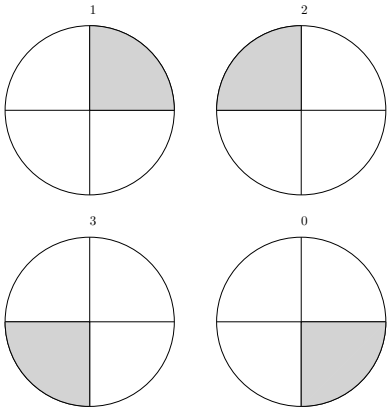

Figure 1: Quotient $\mathbb{Z}_p$ models rotations by $2\pi/p$. Adding p such rotations we arrive at the original situation $0 \in \mathbb{Z}_p$. The Figure represents $\mathbb{Z}_4$. Given any situation the addition of 1 is represented by a rotation by $\pi/2$ in the positive direction.

[12] As the reader might imagine, there is no reasonable algebraic explanation for the imperial system.

[13] When thinking about hours coupled with the am/pm prefixes we actually do a combination of $\mathbb{Z}_2$ and $\mathbb{Z}_{12}$

[14] In particular, whenever we will be talking about a field we will only consider $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, and $\mathbb{Z}_p$, even though all the concerned treatment will hold for any algebraic field (which we have not defined in general).

(vectors) of numbers from $\mathbb{F}$, which we can add, subtract, and multiply by any element of our field $\mathbb{F}$. While all our vector spaces will essentially[15] be of the form $\mathbb{F}^n$, some of our constructions will require us to use a more formal definition.

Definition 2.1. *Let $\mathbb{F}$ be a field. A **vector space** V over field $\mathbb{F}$ is a collection of elements (vectors) equipped with two operations,*

1. *addition $+\colon V \times V \to V$ and*
2. *scalar multiplication $\cdot\colon \mathbb{F} \times V \to V$*

satisfying the following properties:

- *addition is associative, commutative, contains the identity (zero) vector 0, and V contains the opposite element of each vector;*
- *scalar multiplication is compatible, distributive, and normalized.*

Roughly speaking, if we have a collection of vectors we can reasonably add, subtract, and multiply by elements of some field, then this collection forms a vector space.

Example 2.2. *Let $n \in \mathbb{N}$. Given symbols $v_1, \ldots, v_n$ and a field $\mathbb{F}$, all formal*[16] *sums $\sum_{i=1}^n a_i v_i$ where $a_i \in \mathbb{F}$ form a vector space. Operations are defined in the obvious way:*

$$\sum_{i=1}^n a_i v_i + \sum_{i=1}^n a_i' v_i = \sum_{i=1}^n (a_i + a_i') v_i, \quad \text{and} \quad b \sum_{i=1}^n a_i v_i = \sum_{i=1}^n (b a_i) v_i.$$

When $\mathbb{F} = \mathbb{Z}_2$ the corresponding vector space models the power set of $v_1, \ldots, v_n$. A subset $\{v_{i+1}, \ldots, v_{i_k}\}$ corresponds do $v_{i+1} + \ldots + v_{i_k}$. The sum of two formal sums in this setting models the symmetric difference[17] *between the corresponding sets.*

For a prime number p and $n \in \mathbb{N}$ the vector space $(\mathbb{Z}_p)^n = \mathbb{Z}_p^n$ is a finite vector space consisting of p^n elements. While this vector space appear much different than $\mathbb{R}^n$, the formal theory, concepts, and proofs are the same in both cases. We next recast the familiar notions from $\mathbb{R}^n$ in the setting of vector spaces over $\mathbb{F}$.

Let V, W be a vector space over field $\mathbb{F}$.

1. A linear combination of vectors in V is any expression of the form
$$\sum_{i=1}^k a_i v_i, \qquad a_i \in \mathbb{F}, v_i \in V$$
2. A collection of vectors $\{v_1, v_2, \ldots, v_k\} \subset V$ is linearly independent[18] if the only coefficients $a_i \in \mathbb{F}$ satisfying $\sum_{i=1}^k a_i v_i = 0 \in V$ are the zero coefficients, i.e., $a_i = 0, \forall i$.

[15] I.e., up to isomorphism, which will defined later.

☞ Glossary of algebraic properties mentioned in Definition 2.1:

- associativity: $(u+v)+w = u+(v+w), \forall u, v, w \in V$
- commutativity: $u+v = v+u, \forall u, v \in V$
- zero vector: $0+v = v, \forall v \in V$ [it should always be clear from the context whether 0 denotes a number in $\mathbb{F}$ or the zero vector in V]
- the opposite element of $v \in \mathcal{V}$ is denoted by $-v \in V$ and satisfies $v - v = 0$
- compatibility: $(ab)v = a(bv), \forall a, b \in \mathbb{F}, \forall v \in V$
- distributivity: $(a+b)v = av + bv$ and $a(v+w) = av + aw, \forall a, b \in \mathbb{F}, \forall v, w \in V$
- normality: $1 \cdot v = v, \forall v \in V$.

[16] A "formal sum" in this setting means that $v_i + v_j$ is not defined as a single element (as a result of a summation) in a vector space, but is rather thought of as an abstract element in itself. For example, if we want to shop for an apple and a pear, our result should be apple + pear, which does not equal any other single fruit.

[17] The symmetric difference of sets A, B equals $A \cup B \setminus A \cap B$.

☞ Let X be a metric space and $m, n \in \mathbb{N}$. The following are vector spaces over $\mathbb{F}$: the collection of all $m \times n$ matrices with entries in $\mathbb{F}$, the collection of all functions $X \to \mathbb{F}$, the collection of all continuous functions $X \to \mathbb{F}$, the collection of all differentiable functions $X \to \mathbb{F}$ if $\mathbb{F} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, ... Operations on functions in these examples are defined pointwise.

[18] For example, vectors $(1,3)$ and $(2,1)$ are linearly independent in $\mathbb{R}^2, \mathbb{Q}^2, \mathbb{Z}_{13}^2$, but not in $\mathbb{Z}_5^2$.

3. A basis of V is a maximal[19] linearly independent set in V. A a vector space typically has many different bases. However, if V is finite dimensional[20], then the cardinality of each basis is the same. This number is called the dimension of V.

4. A subset $U \subset V$ is a vector subspace [notation: $U \leq V$] of V if it is itself a vector space over $\mathbb{F}$.

5. A map $f\colon V \to W$ is linear if it is additive[21] and multiplicative[22]. A linear map is completely determined[23] by the images of its basis.

6. A bijective linear map is called an isomorphism [notation: $\cong$]. Every vector space over $\mathbb{F}$ of dimension $d \in \mathbb{N}$ is isomorphic to $\mathbb{F}^d$.

7. Let $f\colon V \to W$ be a linear map.

   (a) The kernel of f is defined as

   $$\ker(f) = \{v \in V; f(v) = 0\} \leq V$$

   (b) The image of f is defined as

   $$\mathrm{Im}(f) = \{f(v); v \in V\} \leq W.$$

   The dimension of $\mathrm{Im}(f)$ is called the rank of f.

   (c) Given bases $\{v_1, v_2, \ldots, v_k\}$ of V and $\{w_1, w_2, \ldots, w_l\}$ of W, map f may be represented by an $l \times k$ matrix with entries in $\mathbb{F}$. If $f(v_i) = \sum_{j=1}^{j} a_{i,j} w_j$, then the entry at (j, i) equals $a_{i,j}$.

8. Given a matrix with coefficients in $\mathbb{F}$, we can still preform the Gauss reduction to, for example, compute the rank of a linear map, solve systems of linear equations, ... The procedure is the same as in $\mathbb{R}^n$.

9. Given $U \leq V$, the quotient V/U is defined as the vector space over $\mathbb{F}$ consisting of classes $[v]$ for $v \in V$ under the following identification[24]:

   $$[u] = [v] \Leftrightarrow u - v \in U.$$

   In particular, $[v] = 0$ iff $v \in U$.

Our forthcoming descriptions of holes in simplicial complexes will be expressed in terms of dimensions and bases of vector spaces, for which the following proposition will turn out to be very handy.

[19] In particular, each element of V can be expressed uniquely as a linear combination of the basis vectors.

[20] I.e., if it admits a finite basis.

[21] $f(v + w) = f(v) + f(w), \forall v, w \in V$

[22] $f(av) = af(v), \forall a \in \mathbb{F}, v \in V$

[23] Consequently, a linear map can be represented by a matrix M with coefficients in $\mathbb{F}$ is we chose bases of V and W, with the matrix-vector product $M \cdot v$ representing $f(v)$.

[24] The operations of addition $[u] + [v] = [u + v]$ and multiplication by a scalar $a[u] = [au]$ for $a \in \mathbb{F}, u, v \in V$ are well defined by the same argument that was provided in the previous section for the fields.

Proposition 2.3. *Assume U, V, W are vector spaces over a field $\mathbb{F}$.*

1. *Let $f\colon V \to W$ be a linear map. Then $\operatorname{Im}(f) \cong V/\ker(f)$.*
2. *Let $U \leq V$ be a subspace. Then $\dim(V/U) = \dim(U) - \dim(V)$.*

Proof. 1. Consider the map $g\colon V/\ker(f) \to \operatorname{Im}(f)$ defined by $[u] \mapsto f(u)$. The map is:

- well defined because $[u] = [v] \implies u - v \in \ker(f) \implies f(u - v) = 0 \implies f(u) = f(v) \implies g([u]) = g([v])$;
- surjective by the definitions of $\operatorname{Im} f$ and g;
- injective as $g([u]) = f(u) = 0$ implies $u \in \ker(f)$ and thus $[u] = [0]$.

We conclude that g is an isomorphism.

2. Let $\{w_1, \ldots, w_k\}$ be a basis[25] if U. Complete it by $B_1 = \{v_1, \ldots, v_l\}$ to a basis[26] of V. Observe that $B_2 = \{[v_1], \ldots, [v_l]\}$ is a basis[27] of U/V:

- B_2 is linearly independent: if a linear combination of B_2 was the zero vector in V/U then the corresponding combination of the elements of B_1 was in U. This can only happen if the later combination equals 0 by the choice of B_1 and thus all the coefficients equal 0 by the linear independence of B_1
- B_2 spans the whole V/U because[28] B_1 and U span the whole V.

□

[25] This implies $\dim(U) = k$.

[26] This implies $\dim(V) = k + l$.

[27] This implies $\dim(V) = l$ and thus proves our claim. Furthermore, it demonstrates a way to obtain a basis of U/V.

[28] Take any $v \in V$ and express it as $v = v' + v''$, where $v' \in U$ and v'' is a linear combination of B_1. Then $[v] = [v'']$.

3 Concluding remarks

Recap (highlights) of this chapter

- fields, vector spaces
- quotients and dimension

Background and applications

Fields and abstract vector spaces have a long presence in mathematics going back centuries. Finite fields are attractive for computational implementation for their simplicity, they are easier to handle, computations in them are typically faster than in real numbers, and are resistant to some numerical issues present in reals and floating point computations. Algebraic a predecessor of fields and vector spaces

are (algebraic) groups, another classical subject of algebra, which is now present in virtually every corner of mathematics. Homology of the forthcoming section is typically introduced through groups in the theoretical setting, while the practical aspects of fields motivated exclusive use of fields for practical reasons. A short recap of groups is given in the appendix.

Appendix: A very short introduction to Abelian groups

Many definitions concerning groups are the same as those of fields and vector spaces.

Definition 3.1. *An **Abelian group** $(G,+)$ is a set G with an associative commutative operation $+\colon G\times G\to G$, such that:*

1. *there exists the zero element $0\in G$ satisfying $0+g=g+0, \forall g\in G$;*
2. *for each $g\in G$ there exists its converse $-g\in G$ satisfying $g+(-g)=0$.*

☞ The term "Abelian" refers to commutativity. If the commutativity condition is not satisfied, the structure is called a (non-Abelian) group. These include the groups of permutations (with the operation being the composition) on n elements, the groups of isometries of a metric space (with the operation being the composition), the group of invertible matrices (with the operation being the product), etc.

☞ We will typically shorten $a+(-b)$ to $a-b$.

Examples of Abelian groups include $(\mathbb{R},+),(\mathbb{C},+),(\mathbb{Q},+),(\mathbb{Z},+)$, $(\mathbb{Z}_q,+)$ for any q, $(\mathbb{R}\setminus\{0\},\cdot),(\mathbb{C}\setminus\{0\},\cdot),(\mathbb{Q}\setminus\{0\},\cdot),(\mathbb{Z}_q\setminus\{0\},\cdot)$ for any prime p, etc.

Definition 3.2. *Suppose G,H are Abelian groups. A map $f\colon G\to H$ is a **homomorphism** if $f(a+b)=a(a)+b(b), \forall a,b\in A$. A bijective homomorphism is called an **isomorphism** [notation: $\cong$].*

Suppose G,H are Abelian groups and map $f\colon G\to H$ is a homomorphism.

1. A subset $G'\subset G$ is a subgroup [notation: $G'\leq G$] of G' if it is itself a group.
2. The kernel of f is defined as
$$\ker(f)=\{a\in G;\ f(a)=0\}\leq G$$
3. The image of f is defined as
$$\mathrm{Im}(f)=\{f(a);\ a\in G\}\leq H.$$
4. A collection of elements $a_1,a_2,\ldots,a_k\in G$ is called a generating set[29] of G, if each element of G can be expressed[30] as a sum[31] $\sum_{i=1}^{k} n_i a_i$ for some $n_i\in\mathbb{Z}$.

[29] Or just "generators".

[30] As opposed to vector spaces, such expressions in groups are often not unique, which is why the expression "generating set" is used instead of "basis".

[31] For $n\in\mathbb{N}$ and $a\in G$ we define
$$n\cdot a=\underbrace{a\cdot a\cdot\ldots\cdot a}_{n-times}$$
and $(-n)\cdot a=-(n\cdot a)$.

5. Group G is finitely generated if there exists a finite generating set.

6. If $G' \leq G$, the quotient G/G' is defined as the group consisting of classes $[a]$ for $a \in G$ under the following identification:

$$[a] = [b] \Leftrightarrow a - b \in G'.$$

7. The direct sum of groups G and H is the group denoted by $G \oplus H$ and defined as

$$G \oplus H = \{(a, b);\ a \in G, b \in H\}$$

and the operation being defined coordinate-wise.

A remarkable fact about finitely generated Abelian groups is that the can be classified in a wonderful way.

Theorem 3.3. *[Classification Theorem for finitely generated Abelian groups] Let G be a finitely generated Abelian group. Then there exist :*

- $k, r \in \{0, 1, \ldots\}$,
- $q_1, q_2, \ldots, q_k \in \mathbb{N}$, *and*
- *prime numbers* $p_1, p_2, \ldots, p_k \in \mathbb{N}$,

such that G is isomorphic to

$$\underbrace{\mathbb{Z}^r}_{\text{free part of } G} \oplus \underbrace{\mathbb{Z}_{p_1^{q_1}} \oplus \mathbb{Z}_{p_2^{q_2}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{q_k}}}_{\text{torsion of } G}.$$

Number $r = \mathsf{rank}(G)$ is called the rank of G.

⚠ A comment to Theorem 3.3: A finite Abelian group can, in particular, be decomposed into groups $\mathbb{Z}_{s_i}$, where each s_i is a power of some prime. To see that such a decomposition does not work for other factors of the group cardinality observe that $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_4$, while $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_2$: for each element $a \in \mathbb{Z}_2 \oplus \mathbb{Z}_2$ we have $a + a = 0$, while the same does not hold in $\mathbb{Z}_4$.

Proposition 3.4. *Suppose G, H are Abelian groups, a map $f\colon G \to H$ is a homomorphism, and $G' \leq G$. Then:*

1. $\mathsf{Im}(f) \cong G/\ker(f)$.

2. $\mathsf{rank}(G/G') = \mathsf{rank}(G) - \mathsf{rank}(G')$.