Visual Algebra

Lecture 2.4: Abelian groups

Dr. Matthew Macauley

School of Mathematical & Statistical Sciences
Clemson University
South Carolina, USA
http://www.math.clemson.edu/~macaule/

Abelian groups

Definition

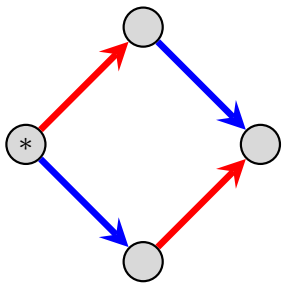
A group G is abelian if $ab = ba$ for all $a, b \in G$.

Remark

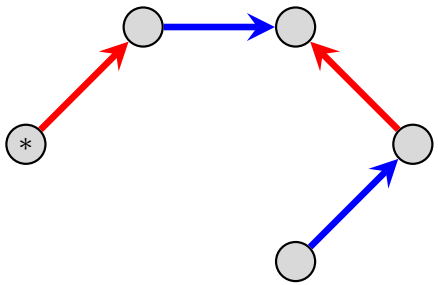
To check that G is abelian, it suffices to only check that $ab = ba$ for all pairs of generators.

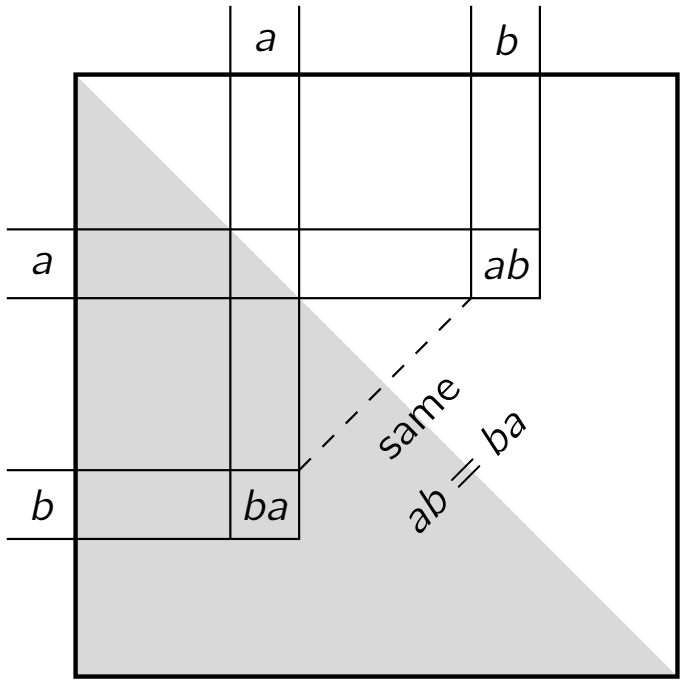
It is easy to check whether a group is abelian from either its Cayley graph or Cayley table.

$ab = ba$



$ab \neq ba$





Direct products

An easy way to construct finite abelian groups is by taking direct products of cyclic groups.

This is an operation that can be done on any collection of groups.

For two groups, A and B, the Cartesian product is the set

$$A \times B = \{(a, b) \mid a \in A,\ b \in B\}.$$

Definition

The direct product of groups A and B is the *set* $A \times B$, and the group operation is done component-wise: if $(a, b), (c, d) \in A \times B$, then

$$(a, b) * (c, d) = (ac, bd).$$

We call A and B the factors.

The binary operations on A and B could be different. For example, in $D_4 \times \mathbb{Z}_4$:

$$(rf, 3) * (r^3, 1) = (rfr^3, 1 + 3) = (r^2 f, 0).$$

These do *not* commute because

$$(r^3, 1) * (rf, 3) = (r^3 rf, 3 + 1) = (f, 0).$$

Direct products of cyclic groups

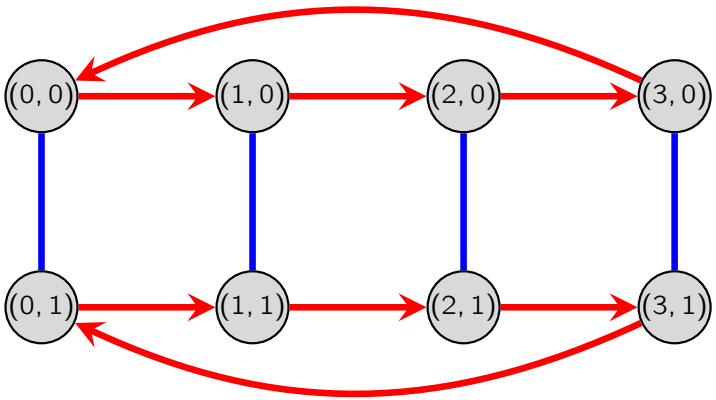
The direct product of $\mathbb{Z}_n$ and $\mathbb{Z}_m$ consists of the set of ordered pairs,

$$\mathbb{Z}_n \times \mathbb{Z}_m = \{(a, b) \mid a \in \mathbb{Z}_n,\ b \in \mathbb{Z}_m\}.$$

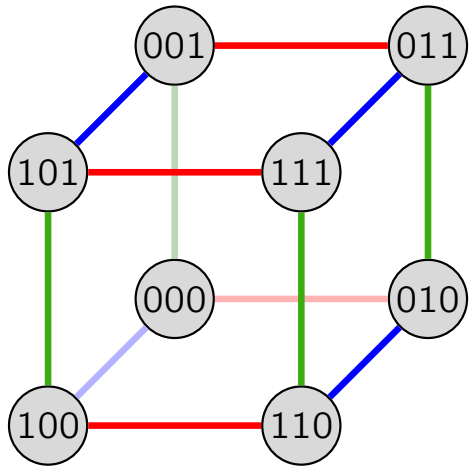
The binary operation is modulo n in the first component, and modulo m in the second component. In other words,

$$(a_1, b_1) + (a_2, b_2) = \big(a_1 + a_2 \pmod{n},\quad b_1 + b_2 \pmod{m}\big).$$

Here are two examples:



$\mathbb{Z}_4 \times \mathbb{Z}_2$

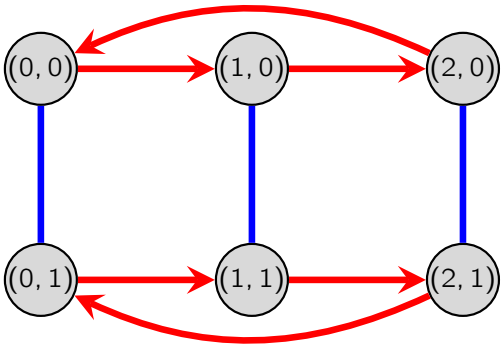


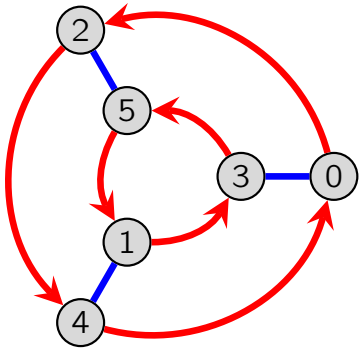
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \textbf{Light}_3$

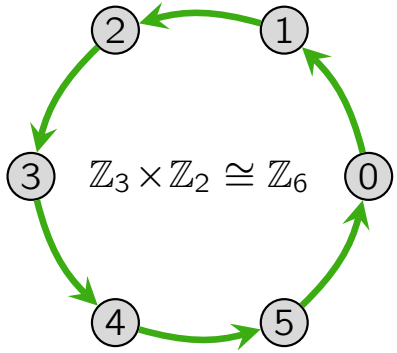
Though $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, we will usually write $V_4 \cong C_2 \times C_2$ since we write V_4 multiplicatively.

Direct products of cyclic groups

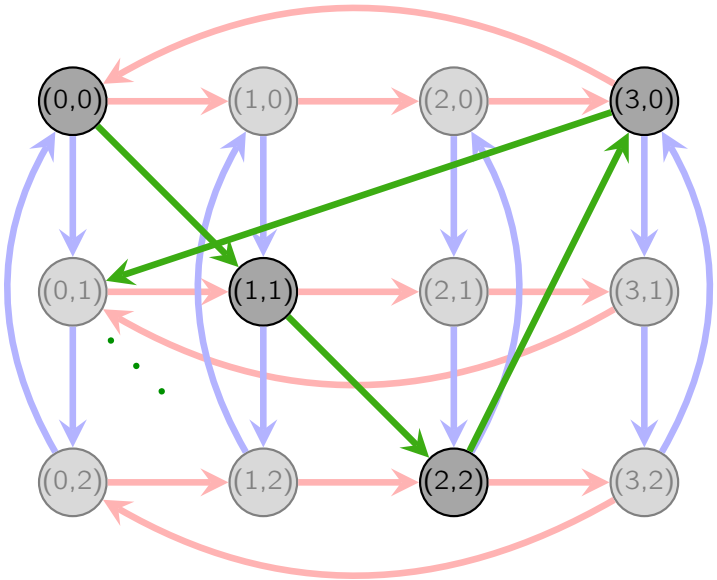
Sometimes, the direct product of cyclic groups is "secretly cyclic."

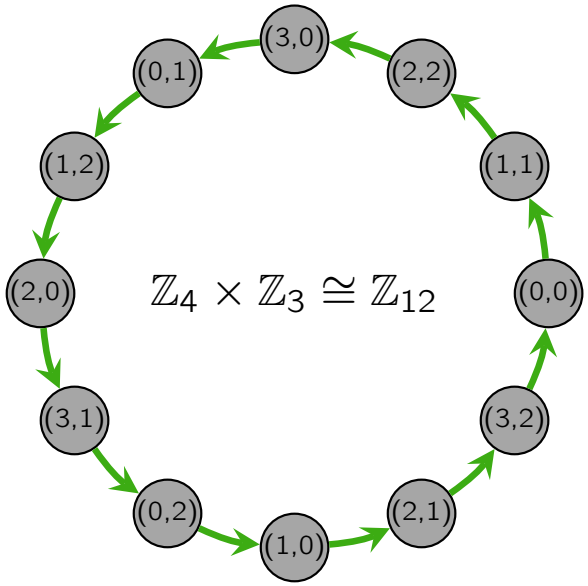






Here is another example:





Direct products of cyclic groups

Proposition

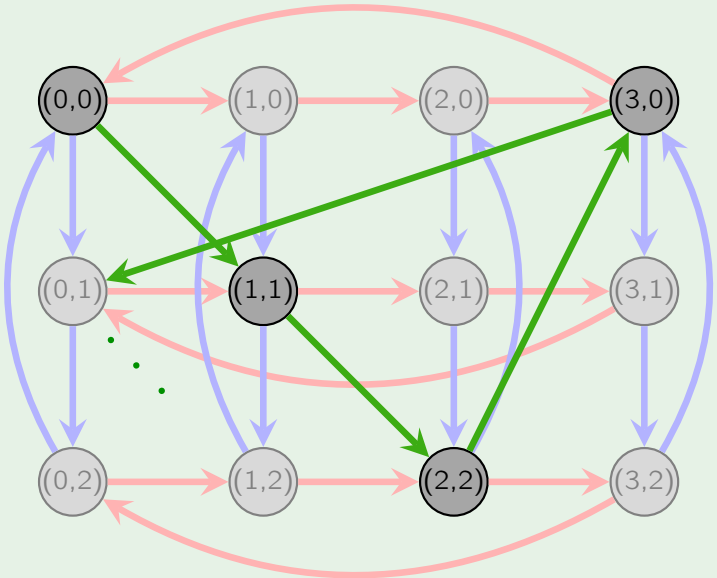
$\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ if and only if $\gcd(n, m) = 1$.

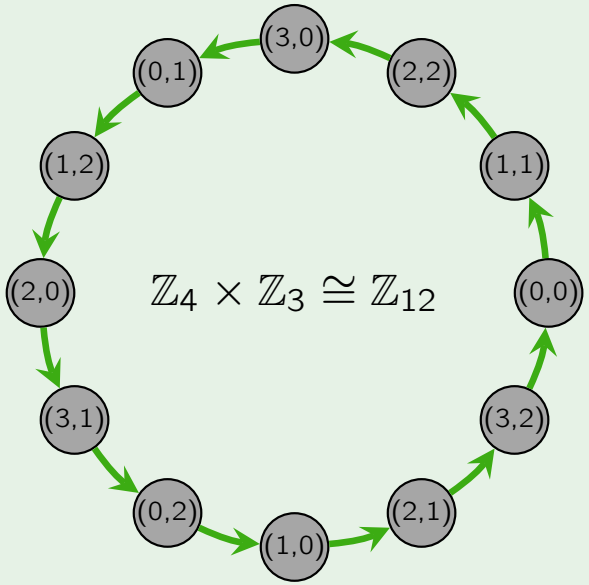
Proof

"$\Leftarrow$": Suppose $\gcd(n, m) = 1$. We claim that $(1, 1) \in \mathbb{Z}_n \times \mathbb{Z}_m$ has order nm.

$|(1, 1)|$ is the smallest k such that "$(k, k) = (0, 0)$." This happens iff $n \mid k$ and $m \mid k$.

Thus, $k = \operatorname{lcm}(n, m) = nm$. ✓





Direct products of cyclic groups

Proposition

$\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ if and only if $\gcd(n, m) = 1$.

Proof (cont.)

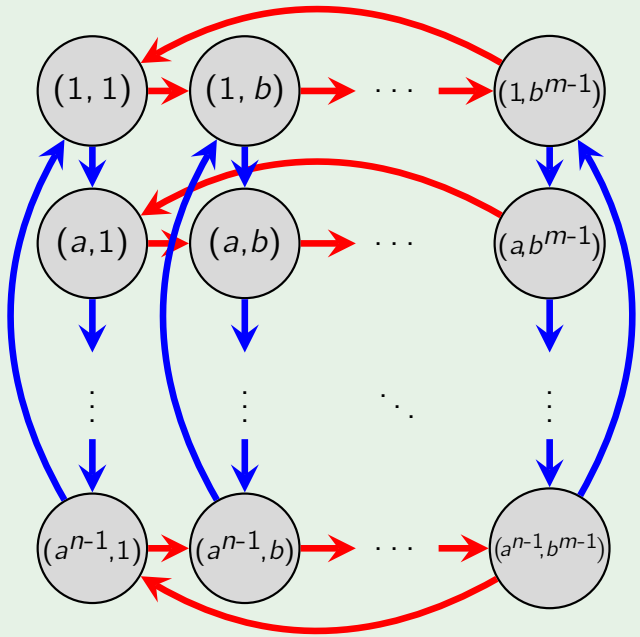
"$\Rightarrow$": Suppose $\mathbb{Z}_n \times \mathbb{Z}_m \times \mathbb{Z}_{nm}$. Then $\mathbb{Z}_n \times \mathbb{Z}_m$ has an element of order nm.

For convenience, we'll switch to "multiplicative notation", and write $C_n \times C_m = \langle (a, b) \rangle$.

Clearly, $\langle a \rangle = C_n$ and $\langle b \rangle = C_m$. Let's look at a Cayley graph for $C_n \times C_m$.

The order of (a, b) must be a multiple of n (the number of rows), *and* of m (the number of columns).

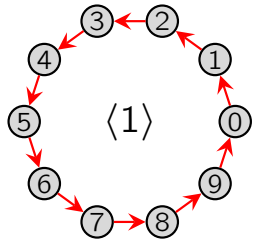
By definition, this is the *least* common multiple of n and m.

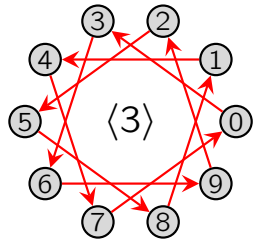


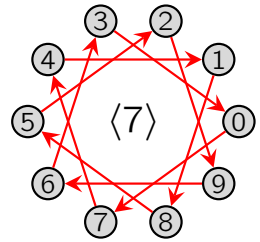
But $|(a, b)| = nm$, and so $\operatorname{lcm}(n, m) = nm$. Therefore, $\gcd(n, m) = 1$. □

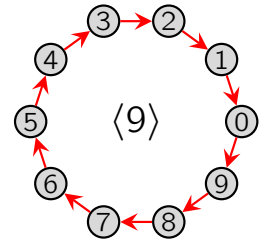
Caveat: cycle graphs need not be unique!

$\mathbb{Z}_{10}$

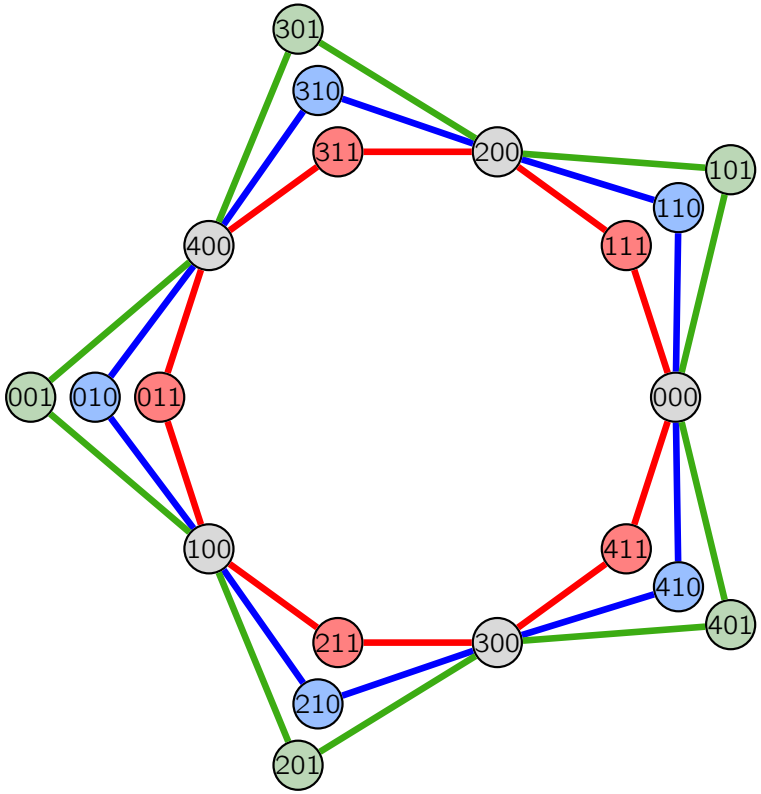


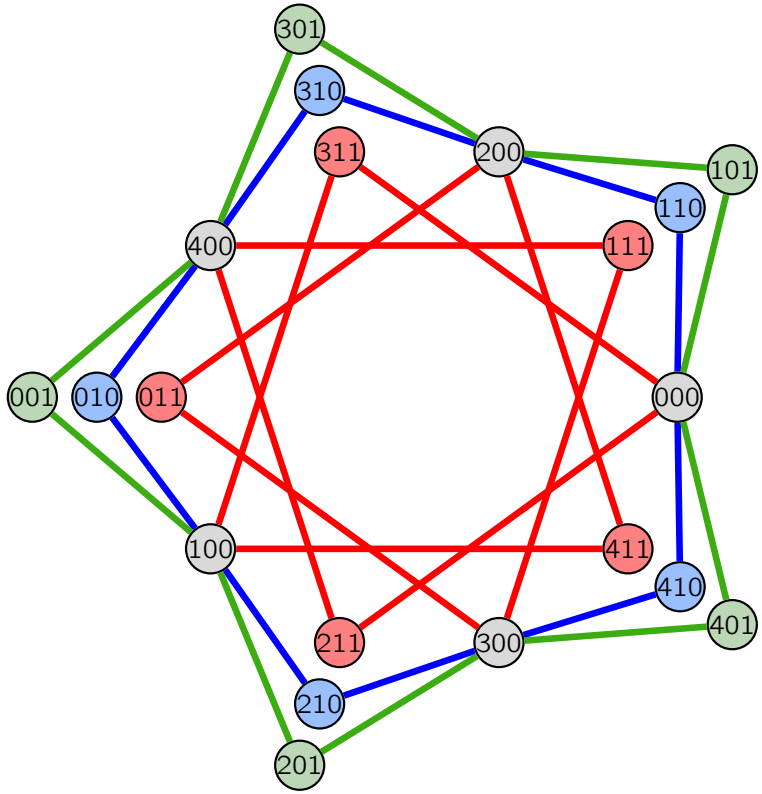






Both of the following are cycle graphs for $\mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.





The fundamental theorem of finite abelian groups

Classification (two different versions)

Every finite abelian group A is isomorphic to a direct product of cyclic groups

$$A \cong \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_m}, \qquad \text{for some } k_1, k_2, \ldots, k_m \in \mathbb{N}, \text{ where}$$

- $k_i = p_i^{d_i}$, for a prime p_i and $d_i \in \mathbb{N}$, ("*prime powers*"), or
- k_i is a multiple of k_{i+1}, ("*elementary divisors*")

Example

Up to isomorphism, there are 6 abelian groups of order $200 = 2^3 \cdot 5^2$:

by "prime-powers"	by "elementary divisors"
$\mathbb{Z}_8 \times \mathbb{Z}_{25}$	$\mathbb{Z}_{200}$
$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$	$\mathbb{Z}_{100} \times \mathbb{Z}_2$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25}$	$\mathbb{Z}_{50} \times \mathbb{Z}_2 \times \mathbb{Z}_2$
$\mathbb{Z}_8 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$\mathbb{Z}_{40} \times \mathbb{Z}_5$
$\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$\mathbb{Z}_{20} \times \mathbb{Z}_{10}$
$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5$	$\mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_2$

The fundamental theorem of finitely generated abelian groups

The classification theorem for *finitely generated* abelian groups is not much different.

Theorem

Every finitely generated abelian group A is isomorphic to a direct product of cyclic groups, i.e., for some integers $n_1, n_2, \ldots, n_m$,

$$A \cong \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{k \text{ copies}} \times \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_m},$$

where each n_i is a prime power, i.e., $n_i = p_i^{d_i}$, where p_i is prime and $d_i \in \mathbb{N}$.

In other words, A is isomorphic to a (multiplicative) group with presentation:

$$A = \left\langle a_1, \ldots, a_k, r_1, \ldots, r_m \mid r_i^{n_i} = 1,\ a_i a_j = a_j a_i,\ r_i r_j = r_j r_i,\ a_i r_j = r_j a_i \right\rangle.$$

Non-finitely generated abelian groups that we are familiar with include:

- The *rational numbers*, $\mathbb{Q}$, under addition
- The *real numbers*, $\mathbb{R}$, under addition
- The *complex numbers*, $\mathbb{C}$, under addition
- all of these (with 0 removed) under multiplication: $\mathbb{Q}^*$, $\mathbb{R}^*$, and $\mathbb{C}^*$.
- the positive versions of these under multiplication: $\mathbb{Q}^+$, $\mathbb{R}^+$ (but not $\mathbb{C}^+$).

Other abelian groups

It is clear that $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$. However, there are many more subgroups of $\mathbb{C}$ than these.

Most of the following are actually rings: additive groups also closed under multiplication. We'll study these more later.

Definition

The Gaussian integers are the complex numbers of the form

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

We'll see $\mathbb{Z}[\sqrt{-m}]$ and others when we encounter rings of algebraic integers.

The set of polynomials in x "*over the integers*" is a group under addition, denoted

$$\mathbb{Z}[x] = \{a_n x^n + \cdots + a_1 x + a_0 \mid a_i \in \mathbb{Z}\}.$$

We can also look at certain subgroups, like the polynomials of degree $\leq n$.

Polynomials can be defined in multiple variables, like

$$\mathbb{Z}[x, y] = \left\{ \sum a_{ij} x^i y^j \mid a_{ij} \in \mathbb{Z}, \text{ all but finitely many } a_{ij} = 0 \right\},$$

or over a finite ring such as $\mathbb{Z}_n$.