# Chapter 1: Geometry, Algebra and Algorithms

~~Polynomials and Affine Space~~

In this chapter, the geometry we are intersted in concerns affine varieties, which are curves and surfaces (and higher dimensional objects) defined by poly! equations. To understand affine varieties, we will need some algebra, and in particular, we will need to study ideals in the polynomial ring $k[x_1, \dots, x_n]$. Finally, we will discuss polynomials in one variable to illustrate the role played by algorithms.

To link algebra and geometry, we will study polynomials over a field. One reason that fields are important is that linear algebra works over any field. In this course, ~~Thes~~ most commonly used fields will be:

- The ~~field of~~ rational numbers $\mathbb{Q}$: the field for most of our computer examples.
- The real numbers $\mathbb{R}$: the field for drawing pictures of curves and surfaces.
- The complex numbers $\mathbb{C}$: the field for proving many of our theorems.

## 1.1. Polynomials and Affine Space

To define polynomials in $n$ variables $x_1, \dots, x_n$ with coefficients in an arbitrary field $k$, we start by defining monomials.

**Def 1.1.1:** A monomial in $x_1, \dots, x_n$ is a product of the form $x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, where all of the exponents $\alpha_1, \dots, \alpha_n$ are nonnegative integers. The total degree of this monomial is the sum $\alpha_1 + \dots + \alpha_n$.

Notation: a) $x^{\alpha} = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ , $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{N}^n$

and $x^{\alpha} = 1$ if $\alpha = (0, 0, \dots, 0)$.

b) $|\alpha| = \alpha_1 + \dots + \alpha_n$

**Def 1.1.2:** A polynomial $f$ in $x_1, \dots, x_n$ with coefficients in $k$ is a finite linear combination (with coefficients in $k$) of monomials. We will write a poly! $f$ in the form

$$f = \sum_{\alpha} a_{\alpha} x^{\alpha}, \quad a_{\alpha} \in k,$$

where the sum is over a finite number of $n$-tuples $\alpha = (\alpha_1, \dots, \alpha_n)$. The set of all polynomials in $x_1, \dots, x_n$ with coefficients in $k$ is denoted $k[x_1, \dots, x_n] = k[\underline{x}]$

Def 1.1.3: Let $f = \sum_{\alpha} a_\alpha x^\alpha$ be a poly$^{!}$ in $k[\underline{x}]$.

i) we call $a_\alpha$ the coefficient of the mononmial $\mathbf{x}^\alpha$.

ii) If $a_\alpha \neq 0$, then we call $a_\alpha x^\alpha$ a term of $f$.

iii) The total degree of $f$, denoted $\deg(f)$, is the maximum $|\alpha|$ such that the coefficient $a_\alpha$ is non-zero.

EX 1.1.4: Consider the polynomials $f = 2x^3y^2z + \frac{3}{2}y^3z^3 - 3xyz + y^2 \in \mathbb{Q}[x,y,z]$

$g = 2x^3y^2 + \frac{3}{2}y^3z^3 - 3xyz + y^2 \in \mathbb{Q}[x,y,z]$.

$\deg(g) = 6$ ~~but~~ Though $\deg(f) = 6$, here there are two ~~poly~~ terms of maximal total degree, which is something that cannot happen for polynomials of one variable.

Note: The set $k[x_1, \dots, x_n] = k[\underline{x}]$ is a commutative ring but it is not a field since $\frac{1}{x_i} \notin k[\underline{x}]$.

Def 1.1.5: Given a field $k$ and a positive integer $n$, we define the n-dimensional affine space over $k$ to be the set

$$k^n = \{(a_1, \dots, a_n) : a_1, \dots, a_n \in k\}.$$

Note: if $n=1$, the affine space is called the affine line
$n=2$, " " plane.

Polynomials are related to affine space. The key idea is that a poly! ~~fun~~ $f = \sum_\alpha a_\alpha x^\alpha \in k[x]$ gives a fun

$$f : k^n \longrightarrow k$$
$$(a_1, \dots, a_n) \mapsto f(a_1, \dots, a_n).$$

Since all of the coefficients also lie in $k$, this operation gives an elt $f(a_1, \dots, a_n) \in k$. What makes a polynomial possible to link algebra and geometry is the ability to regard it as a fun. This dual nature of poly!s has some unexpected consequences. For example, the question " Is $f=0$ ? " now has two potential meanings:

is $f$ the zero poly!?

$$\left[ f = \sum_\alpha a_\alpha x^\alpha = 0 \Rightarrow a_\alpha = 0 \quad \forall \alpha \in \mathbb{N}^n \right]$$

is $f$ the zero function?

$$\left[ f(a_1, \dots, a_n) = 0 \quad \forall (a_1, \dots, a_n) \in k^n \right]$$

The surprizing fact is that these two statements are not equivalent in general as described in the following example.

Consider the set consisting of the two elements 0 and 1, that is, $k = \mathbb{F}_2 = \{0, 1\}$. is a field. Consider the poly! $f = x^2 - x = x(x-1) \in \mathbb{F}_2[x]$.

$f$ is a non-zero poly! but $f(a) = 0 \ \forall a \in \mathbb{F}_2$. which implies that $f$ is the zero fun.

proposition 1.1.6: Let $k$ be an infinite field, and let $f \in k[\underline{x}]$. Then $f = 0$ in $k[\underline{x}]$ iff $f : k^n \to k$ is the zero fun.

proof: $\Rightarrow$) the zero poly! gives the zero fun ✓

$\Leftarrow$) Induction on the number of variables $n$. When $n = 1$, it is well known that a non zero poly! in $k[x]$ of degree $m$ has at most $m$ distinct roots. If $f(a) = 0 \ \forall a \in k$, $f$ has infinitely many roots since $k$ is infinite. thus $f$ must be the zero polynomial. Now assume that the converse is true for $n-1$, and let $f \in k[\underline{x}]$ be a poly! that vanishes at all points of $k^n$. By collecting the various powers of $x_n$, we can write $f$ in the form

$$f = \sum_{i=0}^{N} g_i(x_1, \dots, x_{n-1})\, x_n^i,$$

where $g_i \in k[x_1, \dots, x_{n-1}]$. We will show that each $g_i$

is the zero polynomial in $n-1$ variables, which will force $f$ to be the zero in $k[\underline{x}]$.

Fix $(a_1,\dots,a_{n-1}) \in k^{n-1}$, then we have

$$f(a_1,\dots,a_{n-1},x_n) \in k[x_n].$$

By our hypothesis on $f$, $f(a_n)=0$ $\forall a_n \in k$. It follows from the case $n=1$ that $f(a_1,\dots,a_{n-1},x_n)$ is the zero poly! in $k[x_n]$.

$$f(a_1,\dots,a_{n-1},x_n)=0 \Rightarrow g_i(a_1,\dots,a_{n-1})=0$$

Since $(a_1,\dots,a_{n-1})$ was arbitrarily chosen in $k^{n-1}$, it follows that each $g_i \in k[x_1,\dots,x_{n-1}]$ gives the zero function on $k^{n-1}$! Our inductive assumption then implies that each $g_i$ is the zero poly! in $k[x_1,\dots,x_{n-1}]$. Thus

$f$ is the zero poly! in $k[\underline{x}]$.

Corollary 1.1.7: Let $k$ be an infinite field, and let $f,g \in k[x_1,\dots,x_n]$. Then $f=g$ in $k[x_1,\dots,x_n]$ iff $f: k^n \to k$ and $g: k^n \to k$ are the same function.

proof

($\Rightarrow$) clear

($\Leftarrow$) $f,g \in k[\underline{x}]$ give the same fun on $k^n$, that is,

$$f(a)=g(a) \quad \forall a \in k^n$$

$$\Rightarrow f(a)-g(a) = (f-g)(a)=0 \quad \forall a \in k^n$$

$$\Rightarrow f-g=0 \text{ by prop 1.1.6.}$$

## 1.2: Affine Varieties

Def 1.2.1: Let $k$ be a field, and let $f_1, \dots, f_s$ be polyls in $k[\underline{x}]$. Then we set

$$V(f_1, \dots, f_s) = \{ (a_1, \dots, a_n) \in k^n \mid f_i(a_1, \dots, a_n) = 0, \ \forall\ 1 \le i \le s \}$$

We call $V(f_1, \dots, f_s)$ the affine variety defined by $f_1, \dots, f_s$.

▷ An affine variety $V(f_1, \dots, f_s) \subset k^n$ is the set of all solutions of the system of equations $f_i(\underline{x}) = 0$ for $1 \le i \le n$.

We will use the letters $V$, $W$, etc to denote affine varieties.

EX 1.2.2:

① The variety defined by the polyl

$$f = x^2 + y^2 - 1 \in \mathbb{R}[x, y]$$

is the circle of radius 1 centered at the origin. That is,

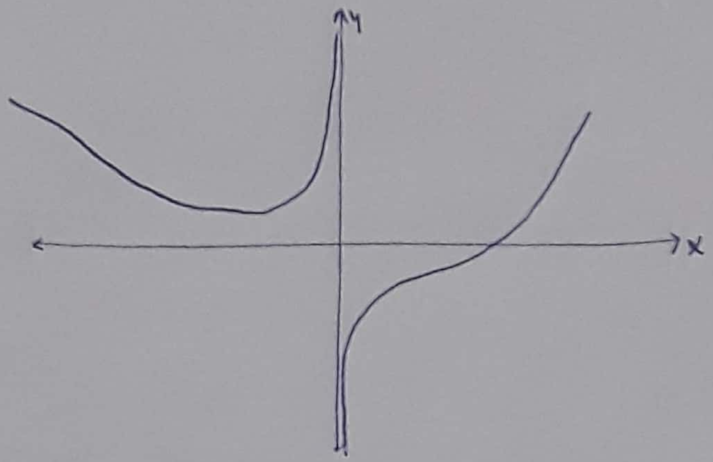
$$V(f) = \{ (x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1 \}$$

② The conic sections in ~~alge~~ analytic geometry such as circles, ellipses, parabolas, and hyperbolas are affine varieties.

③ Graphs of polyl functions are affine varieties [the graph of $y = f(x)$ is $V(y - f(x))$]

(4) graphs of rational functions are affine varieties.

For example, consider the graph of $y = \frac{x^3-1}{x}$:




points in this graph are points in the affine variety $V(xy - x^3+1)$.

(5) Consider the poly! $f = z - x^2 - y^2 \in \mathbb{R}[x,y,z]$.

A nice affine variety defined by is given by paraboloid of revolution $V(z-x^2-y^2) = V(f)$, which is obtained by rotating the parabola $z = x^2$ about the $z$-axis.

(6) a) $V(z^2 - x^2 - y^2) \rightarrow$ Cone

b) $V(x^2 - y^2z^2 + z^3) \rightarrow$ Surface.

(7) A curve in $\mathbb{R}^3$ called the twisted cubic, which is the variety $V(y - x^2, z - x^3)$.

## Basic properties of Affine varieties

Lemma 1.2.3: If $V, W \subset k^n$ are affine varieties, then so are $V \cup W$ and $V \cap W$.

proof:- Suppose that $V = V(f_1, \ldots, f_s)$ and $W = V(g_1, \ldots, g_t)$. Then we claim that

(i) $V \cap W = V(f_1, \ldots, f_s, g_1, \ldots, g_t)$

(ii) $V \cup W = V(f_i g_j \mid 1 \le i \le s, 1 \le j \le t)$.

(i) Let $a \in V \cap W$. Then $f_i(a) = g_j(a) = 0 \quad \forall \ 1 \le i \le s, 1 \le j \le t$.

$\Rightarrow a \in V(f_1, \ldots, f_s, g_1, \ldots, g_t)$

and let $a \in V(f_1, \ldots, f_s, g_1, \ldots, g_t)$. Then

$f_i(a) = 0$ and $g_j(a) = 0 \quad \forall \ 1 \le i \le s, 1 \le j \le t$

$\Rightarrow a \in V(f_1, \ldots, f_s)$ and $a \in V(g_1, \ldots, g_t)$

$\Rightarrow a \in V \cap W$

(ii) $a \in V \Rightarrow f_i(a) = 0 \quad \forall \ 1 \le i \le s$

$\Rightarrow f_i(a) g_j(a) = 0 \quad \forall \ 1 \le i \le s, 1 \le j \le t$

$\Rightarrow a \in V(f_i g_j)$ ~~and a~~

Thus $V \subset V(f_i g_j)$ and $W \subseteq V(f_i g_j)$

$\Rightarrow V \cup W \subseteq V(f_i g_j)$

$a \in V(f_i g_j) \Rightarrow \overset{a \in V}{} \; a \in V \cup W$

Suppose $a \notin V$. Then $f_{i_0}(a) \neq 0$ for some $i_0$.

Since $f_{i_0} g_j(a) = 0 \;\; \forall j$, $g_j(a) = 0 \;\; \forall j$

$\Rightarrow a \in W \Rightarrow a \in V \cup W$ $\boxed{\text{II}}$

EX 1.2.4: Consider the union of the $(x,y)$-plane and the $z$-axis in affine 3-space. By the above formula, we have

$$V(z) \cup V(x,y) = V(zx, zy)$$

II Lemma 1.2.3 implies that finite intersections and unions of affine varieties are again affine varieties.

Some interesting questions concerning affine varieties

Suppose that we have $f_1, \ldots, f_s \in k[x]$.

1. Consistency: Can we determine if $V(f_1, \ldots, f_s) \neq \phi$? That is, do the equations $f_1 = \cdots = f_s = 0$ have a common solution?

2. Finiteness: Can we determine if $V(f_1, \ldots, f_s)$ is finite, and if so, can we find all of the solutions explicitly?

3. Dimension: Can we determine the "dimension" of $V(f_1, \ldots, f_s)$?

The answer to the above questions is yes, although care must be taken in choosing the field $k$ that we work over. Later, in this lecture, we will give complete sol$^n$s to all three problems.

## 1.3: Parametrizations of Affine Varieties

In this section, the problem of describing the points of an affine variety $V(f_1, \ldots, f_s)$ will be discussed.

Given polynomials $f_1, \ldots, f_s \in k[x]$ with coeffs in a field $k$. When there are finitely many sol$^n$s for the systems of poly$^l$ equations $f_i = 0$ $1 \leq i \leq s$, we simply list them all. But what do we do when there are infinitely many? This question leads to the notion of parametrizing an affine variety.

We start with the following examples:

Ex 1.3.1: Let the field be $\mathbb{R}$, and consider the system of equations $x+y+z=1$ and $x+2y-z=3$ $\rightarrow (1)$
Geometrically, this represents the line in $\mathbb{R}^3$, which is the intersection of the planes $x+y+z=1$ & $x+2y-z=3$. These equations have finitely many sol$^n$s. To describe the sol$^n$s, we use row operations on equ$^n$s (1) to obtain the equivalent equations

$$x+3z=-1 \quad \text{and} \quad y-2z=2.$$

Letting $z=t$, where $t$ is arbitrary, this implies that all sol$^n$s (1) are given by

$$x = -1-3t, \quad y = 2+2t, \quad z = t \rightarrow (2)$$

as $t$ varies over $\mathbb{R}$. We call $t$ a parameter, and (2) is, thus, a parametrization of the sol$^{ns}$ of (1).

Ex 1.3.2: How do we describe points in $V(x^2+y^2-1)$.

Sol$^n$: A common way to parametrize the circle is using trigonometric fun$^c$ctions:

$$x = \cos(t) \quad \text{and} \quad y = \sin(t).$$

An algebraic way to parametrize this circle is

$$x = \frac{1-t^2}{1+t^2} \quad \text{and} \quad y = \frac{2t}{1+t^2}$$

Def 1.3.3: Let $k$ be a field. A rational function in $t_1, \ldots, t_m$ with coefficients in $k$ is a quotient $f/g$ of two polynomials $f, g \in k[\underline{t}]$ where $g$ is not the zero poly$^n$. Furthermore, two rational functions $f/g$ and $h/k$ are equal, provided that $kf = gh$ in $k[\underline{t}]$. Finally, the set of all rational functions in $t_1, \ldots, t_m$ with coefficients in $k$ is denoted $k(\underline{t})$.

Exercise: Show that $k(\underline{t})$ is a field.

▷ Suppose that we are given a variety $V = V(f_1, \ldots, f_s) \subset k^n$. Then a rational parametric representation of $V$ consists of rational functions $r_1, \ldots, r_n \in k(\underline{t})$ such that the points given by

$x_1 = r_1(t), \ldots, x_n = r_n(t)$ lie in $V$.

Moreover, we require that $V$ to be the "smallest" variety containing these points.

Note: A parametrization may not cover all points of $V$. See, for example, parametrization of the above circle.

▷ In many situations, we have a parametrization of a variety $V$, where $r_1, \ldots, r_n$ are polynomials rather than rational functions. This is what we call a polynomial parametric representation of $V$. By contrast, the original defining equations $f_1 = \cdots = f_s = 0$ of $V$ are called an implicit representation of $V$.

▷ One of our main virtues of a parametric representation of a curve or surface is that it is easy to draw on a computer. Given the formulas for the parametrization, the computer evaluates them for various values of the parameters and then plots the resulting points.

EX 1.3.4: Consider the surface $V(x^2-y^2z^2+z^3)$: The implicit representation is $x^2-y^2z^2+z^3=0$. To draw the surface, we use the parametric representation given by

$x = t(u^2-t^2)$, $y = u$, $z = u^2-t^2$.

[use $-1 \leq t, u \leq 1$]

Question: Does this parametrization covers the entire surface $V = V(x^2 - y^2z^2 + z^3)$?

11) Suppose we want to know whether or not a point $(a,b,c)$ is on the above surface $V$: In this case, it is often useful to have an implicity representation of ~~v~~ a variety. For example,

Is the point $(1,2,-1) \in V$?

Ans Using the implicit representation of $V$, we can easily see that $1^2 - 2^2(-1)^2 + (-1)^3 = 1-4-1 = -4 \neq 0$, the point is not on the surface. In other words, the system of equations $1 = t(u^2 - t^2)$, $2 = u$, $-1 = u^2 - t^2$ have no solutions.

The Desirability of having both types of representations leads to the following two questions:

a) Parametrization: Does every affine variety have a rational parametric representation?

b) Implicitization: Given a parametric representation of an affine variety, can we ~~defined~~ the defining equations, that is, can we find an implicit representation?

# Chapter 2: The structure of Groups

## 1. Free Abelian Groups

Def 2.1: A basis of an abelian group $F$ is a subset $X$ of $F$ such that

i) $F = \langle X \rangle$

ii) for distinct $x_1, x_2, \ldots, x_k \in X$ and $n_i \in \mathbb{Z}$,

$$n_1 x_1 + n_2 x_2 + \cdots + n_k x_k = 0 \Rightarrow n_i = 0 \text{ for every } i.$$

Them 2.2: The ff conditions on an abelian group $F$ are equivalent:

i) $F$ has a nonempty basis.

ii) $F$ is the internal direct sum of a family of infinite cyclic subgroups.

iii) $F$ is (isomorphic to) a direct sum of copies of the additive group $\mathbb{Z}$ of integers

iv) There exists a non-empty set $X$ and a fun $i : X \to F$ with the ff property: given an abelian group $G$ and fun $f : X \to G$, there exists a unique hsm of groups $\bar{f} : F \to G$ such that $\bar{f} i = f$.

Def 2.3: An abelian group F that satisfies the condition of Thm 2.2 is called a free abelian group (on the set X).

By defn the trivial group 0 is the free abelian group on the null set $\phi$.

Thm 2.4: Any two bases of a free abelian group F have the same cardinality.

The cardinal no of any basis X of the free abelian group F is thus an invariant of F; $|X|$ is called the rank of F.

proposition 2.5: Let $F_1$ be the free abelian group on the set $X_1$ and $F_2$ the free abelian group on the set $X_2$. Then $F_1 \cong F_2$ iff $F_1$ and $F_2$ have the same rank (that is, $|X_1| = |X_2|$)

Thm 2.6: Every abelian group G is the homomorphic image of a free abelian group of rank $|X|$, where X is a set of generators of G.

Lemma 2.7: If $\{x_1, \dots, x_n\}$ is a basis of a free abelian group F and $a \in \mathbb{Z}$, then for all $i \neq j$,

$\{x_1, \dots, x_{j-1}, x_j + a x_i, x_{j+1}, \dots, x_n\}$ is also a basis of F.

Proof :- Since $x_j = -ax_i + (x_j + ax_i)$. it follows that

$F = \langle x_1, \ldots, x_{j-1}, x_j + ax_i, x_{j+1}, \ldots, x_n \rangle$

$k_1 x_1 + k_j x_{j-1} + k_j(x_j + ax_i) + k_{j+1} x_{j+1} + \cdots + k_n x_n = 0$

$\Rightarrow k_1 x_1 + \cdots + \underline{k_i x_i} + k_{j-1} x_{j-1} + k_j x_j + k_j a x_i + k_{j+1} x_{j+1} + \cdots + k_n x_n = 0$

$\Rightarrow k_1 x_1 + \cdots + (k_i + k_j a) x_i + \cdots + k_j x_j + \cdots + k_n x_n = 0$

$\Rightarrow k_1 = 0 \quad k_i + k_j a = 0 \quad k_j = 0, k_n = 0$

$\Rightarrow k_i = -k_j a = k_i = 0$ ✓

$\therefore k_t = 0 \quad \forall t$

Thm 2.8: If $F$ is a free abelian group of finite rank $n$ & $G$ is a nonzero subgroup of $F$, then there exists a basis $\{x_1, \ldots, x_n\}$ of $F$, an integer $r$ $(1 \le r \le n)$ and positive integers $d_1, \ldots, d_r$ such that $d_1 \mid d_2 \mid \cdots \mid d_r$ and $G$ is free abelian with basis $\{d_1 x_1, \ldots, d_r x_r\}$.

Remark 2.9: Every subgroup of a free abelian group of (possibly infinite) rank $m$ is free of ~~abelian of~~ rank at most $m$.

Corollary 2.10: If $G$ is a finitely generated abelian group generated by $n$ elts, then every subgroup $H$ of $G$ may be generated by $m$ elements with $m \leq n$.

2. Finitely Generated Abelian Groups

Thm 2.11: Every finitely generated abelian group $G$ is (isomorphic to) a finite direct sum of cyclic groups in which the finite cyclic summands (if any) are of orders $m_1, \dots, m_t$, where $m_1 > 1$ & $m_1 | m_2 | \dots | m_t$.

$$\left[ \; G \cong Z_{m_1} \oplus \cdots \oplus Z_{m_t} \oplus (Z \oplus \cdots \oplus Z) \right.$$

where $m_1 > 1$, $m_1 | m_2 | \dots | m_t$ and $(Z \oplus \cdots \oplus Z)$ has rank $s$ ]

Or $\quad G \cong Z \oplus \cdots \oplus Z$

Thm 2.12: Every f.g abelian group $G$ is (isomorphic to) a finite direct sum of cyclic groups, each of which is **either** infinite or of order a power of a prime.

Lemma 2.13: Let $m$ be a positive integer and let $m = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ ($p_1, \dots, p_t$ distinct primes and each $n_i > 0$), then

$$Z_m \cong Z_{p_1^{n_1}} \oplus Z_{p_2^{n_2}} \oplus \cdots \oplus Z_{p_t^{n_t}}$$

④ ③

Remark 2.14: Let m and n be positive integers such that m and n are coprime, then

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$$

EX 2.15: $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5$

$\mathbb{Z}_{36} \cong \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^2} = \mathbb{Z}_4 \oplus \mathbb{Z}_9$

proof: $\varphi_1 : \mathbb{Z}_m \longrightarrow \mathbb{Z}_{mn}$ → monosm
$k \longmapsto nk$

$\varphi_2 : \mathbb{Z}_n \longmapsto \mathbb{Z}_{mn}$ monosm
$k \longmapsto mk$

$\varphi : \mathbb{Z}_m \oplus \mathbb{Z}_n \longrightarrow \mathbb{Z}_{mn}$

$(x, y) \longmapsto \varphi_1(x) + \varphi_2(y) = nx + my$

is a well-defined hsm.

Since $(m, n) = 1$, $\exists\, a, b \in \mathbb{Z}$ $\ni$

$am + nb = 1$

$\Rightarrow$ $k = amk + nbk = \varphi(bk, ak)$ $\forall k \in \mathbb{Z}_{mn}$

$\Rightarrow \varphi$ is an epsm

$\varphi(x_1, y_1) = \varphi(x_2, y_2)$

$\Rightarrow$ $nx_1 + my_1 = nx_2 + my_2 \Rightarrow n(x_1 - x_2) = m(y_2 - y_1)$

$\Longleftrightarrow$ $x_1 - x_2 = mk$ and $y_2 - y_1 = nk$ for some $k \in \mathbb{Z}$

Scanned by CamScanner

$\Rightarrow x_1 \equiv x_2 \mod m$ and $y_2 \equiv y_1 \mod n$

so $(x_1, y_1) = (x_2, y_2)$ in $\mathbb{Z}_m \oplus \mathbb{Z}_n$

Thus, $\varphi$ is 1-1 and, hence,

$$\mathbb{Z}_n \oplus \mathbb{Z}_m \cong \mathbb{Z}_{mn}.$$

Corollary 2.16: If $G$ is a finite $\boxed{\text{abelian}}$ group, of order $n$, then $G$ has a subgroup of order $m$ for every positive integer $m$ that divides $n$.

Remark 2.17: Corollary 2.16 may be false if $G$ is not abelian.

Lemma 2.18: Let $G$ be an abelian group, $m$ an integer and $p$ a prime integer. Then each of the ff is a subgroup of $G$:

i) $mG = \{mu \mid u \in G\}$

ii) $G[m] = \{u \in G \mid mu = 0\}$

iii) $G(p) = \{u \in G \mid |u| = p^n \text{ for some } n \geq 0\}$

iv) $G_t = \{u \in G \mid |u| \text{ is finite}\}$

In particular, there are isomorphisms

v) $\mathbb{Z}_{p^n}[p] \cong \mathbb{Z}_p$ $(n \geq 1)$ and $p^m \mathbb{Z}_{p^n} \cong \mathbb{Z}_{p^{n-m}}$

$(m < n)$

Let $H$ and $G_i$ $(i \in I)$ be abelian groups.

vi) If $g: G \to \sum_{i \in I} G_i$ is an isomorphism, then the restrictions of $g$ to $mG$ and $G[m]$ respectively are isomorphisms $mG \cong \sum_{i \in I} mG_i$ and

$G[m] \cong \sum_{i \in I} G_i[m]$.

vii) If $f: G \to H$ is an isomorphism, then the restrictions of $f$ to $G_t$ and $G(p)$ respectively are isomorphisms $G_t \cong H_t$ and $G(p) \cong H(p)$.

proof:- (i) Since $me = me \in mG \Rightarrow mG \neq \phi$

Let $x, y \in mG$. Then $x = mu_1$ and $y = mu_2$, $u_1, u_2 \in G$

$xy^{-1} = (mu_1)(mu_2)^{-1} = mu_1 u_2^{-1} m^{-1} = u_1 u_2^{-1}$ ($\because G$ is abelian)

$= u_1 u_2^{-1} \in G$ ($\because G$ is a group)

Def 2.19:- Let $G$ be an abelian group.

a) The subgroup $G_t$ defined in Lemma 2.5 is called the torsion subgroup of $G$.

b) If $G = G_t$, then $G$ is said to be a torsion group.

(c) If $G_t = 0$, then $G$ is said to be torsion free.

Thm 2.20: Let $G$ be a f.g abelian group.

i) There is a unique nonnegative integer $s$ such that the number of infinite cyclic summands in any decomposition of $G$ as a direct sum of cyclic groups is precisely $s$;

ii) either $G$ is free abelian or there is a unique list of (not necessarily distinct) positive integers $m_1, \dots, m_t$ such that $m_1 > 1$, $m_1 | m_2 | \dots | m_t$ and

$$G \cong \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_t} \oplus F$$

with $F$ free abelian

iii) either $G$ is free abelian or there is a list of positive integers $p_1^{n_1}, \dots, p_k^{n_k}$ which is unique except for the order of its members, such that $p_1, \dots, p_k$ are (not necessarily distinct) primes, $s_1, \dots, s_k$ are (not necessarily distinct) positive integers and

$$G \cong \mathbb{Z}_{p_1^{s_1}} \oplus \dots \oplus \mathbb{Z}_{p_k^{s_k}} \oplus F$$

with $F$ free abelian.

Def 2.21: If $G$ is a f.g abelian group, then (a) the uniquely determined integers $m_1, \dots, m_t$ as in Thm 2.20(ii) are called the invariant factors of $G$.

(b) the uniquely determined prime powers as in Thm 2.20(iii) are called the elementary divisors of $G$.

EX 2.21: Let G be a finite abelian group of order 1500.

Find (a) Elementary divisors of G

(b) Invariant factors of G.

Soln: The Group G may be determined up to Ism as follows:
Since the product of the elementary divisors of a finite group G must be $|G|$ & $1500 = 2^2 \cdot 3 \cdot 5^3$, the only possible families of elementary divisors are

$$\{2, 2, 3, 5^3\}, \{2, 2, 3, 5, 5^2\}, \{2, 2, 3, 5, 5, 5\}$$
$$\{2^2, 3, 5^3\}, \{2^2, 3, 5, 5^2\}, \{2^2, 3, 5, 5, 5\}$$

Each of these six families determines an abelian group of order 1500.

EX: $\{2, 2, 3, 5^3\}$ determines $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{125}$

By Thm 2.12 every abelian group of order 1500 is isomorphic to one of these six groups & no two of these six are isomc by the ff corollary:

Corollary 2.22: Two f.g abelian groups G and H are isomc iff $G/G_t$ & $H/H_t$ have the same rank and G and H have the same invariant factors (resp. elementary divisors).

Note: If the invariant factors $m_1, \dots, m_t$ of a f.g abelian group $G$ are known, then the elementary divisors of $G$ are the prime powers $p^n$ $(n>0)$ which appear in the prime factorization of $m_1, \dots, m_t$.

: If the elementary divisors of $G$ are known, they may be arranged in the ff way (after the insertion of some terms of the form $p^0$ if necessary):

$$p_1^{n_{11}}, \quad p_2^{n_{12}}, \dots, p_r^{n_{1r}}$$

$$p_1^{n_{21}}, \quad p_2^{n_{22}}, \dots, p_r^{n_{2r}}.$$

$$\vdots$$

$$p_1^{n_{t1}}, \quad p_2^{n_{t2}}, \dots, p_r^{n_{tr}}$$

where $p_1, \dots, p_r$ are distinct primes for each $j = 1, \dots, r$, $0 \le n_{1j} \le n_{2j} \le \dots \le n_{tj}$ with some $n_{tj} \neq 0$ and finally $n_{1j} \neq 0$ for some $j$

EX 2.22: Consider the group $G = \mathbb{Z}_5 \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{36} \oplus \mathbb{Z}_{54}$.

Find (a) Elementary divisors of $G$

(b) invariant factors of $G$

Soln: By Lemma 2.13 $\mathbb{Z}_{15} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_5$,

$\mathbb{Z}_{25} \cong \mathbb{Z}$ $\mathbb{Z}_{36} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_9$, $\mathbb{Z}_{54} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{27}$

$\Rightarrow G \cong \mathbb{Z}_5 \oplus (\mathbb{Z}_5 \oplus \mathbb{Z}_3) \oplus \mathbb{Z}_{25} \oplus (\mathbb{Z}_9 \oplus \mathbb{Z}_4) \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_{27})$.

Hence, the elementary divisors ~~are~~ of G are

$2, 2^2, 3, 3^2, 3^3, 5, 5, 5^2$ which may be arranged as explained above

$$\begin{array}{ccc} 2^0 & 3 & 5 \\ 2^1 & 3^2 & 5^2 \\ 2^2 & 3^3 & 5^2 \end{array}$$

$\Rightarrow$ the invariant factors are $2^0 \times 3 \times 5 = 15$, $2 \cdot 3^2 \cdot 5 = 90$ and $2^2 \cdot 3^3 \cdot 5^2 = 2700$ so that

$$G \cong \mathbb{Z}_{15} \oplus \mathbb{Z}_{90} \oplus \mathbb{Z}_{2700}$$

clearly, $15 \mid 90 \mid 2700$

## 2.3: The Sylow Theorems

The Sylow Theorems are a basic first step in understanding the structure of an arbitrary finite group.

Lemma 2.23: If a group H of order $p^n$ ($p$ prime) is

Thm 2.23: [Cauchy]
If G is a finite group whose order is divisible by a prime p, then G contains an elt of order p.

**Def 2.24:** A group in which every element has order a power ($\geq 0$) of some fixed prime $p$ is called a $p$-group.

**Def 2.25:** If $H$ is a subgroup of a group $G$ and $H$ is a $p$-group, $H$ is said to be a $p$-subgroup of $G$.

**Ex 2.26:** $H = \langle e \rangle < G$ (a group).
$H$ is a $p$-subgroup of $G$ for every prime $p$ since
$\underline{\underline{|H| = 1 = p^0}}$

**Corollary 2.27:** A finite group $G$ is a $p$-group iff $|G|$ is a power of $p$.

~~Ex 2.28:~~ ~~$G = (\mathbb{Z}_4, +)$~~ ~~$|G| = 4$~~

**Thm 2.28** [First Sylow Theorem]
Let $G$ be a group of order $p^n m$, with $n \geq 1$, $p$ prime and $(p, m) = 1$. Then $G$ contains a subgroup of order $p^i$ for each $1 \leq i \leq n$ and every subgroup of $G$ of order $p^i$ ($i < n$) is normal in some subgroup of order $p^{i+1}$.

~~Def 2.24: Let $G$ be a group and let $p$ be a prime~~

~~1. A group of order $p$~~

Defn 2.29: A subgroup $H$ of a group $G$ is said to be a Sylow $p$-subgroup ($p$ prime) if $H$ is a maximal $p$-subgroup of $G$ (that is, $H < H' < G$ with $H'$ a $p$-group implies $H = H'$).

Note: (a) Sylow $p$-subgroups always exist, though they may be trivial

(b) Every $p$-subgroup is contained in a Sylow-$p$ subgroup

(c) A finite group $G$ has a non-trivial Sylow $p$-subgroup for every prime $p$ that divides $|G|$.

Corollary 2.30: Let $G$ be a group of order $p^n m$ with $p$ prime, $n \geq 1$ and $(m, p) = 1$. Let $H$ be a $p$-subgroup of $G$.

i) $H$ is a sylow $p$-subgroup of $G$ iff $|H| = p^n$.

ii) If there is only one Sylow $p$-subgroup $P$, then $P$ is normal in $G$.

Thm 2.31: [$2^{nd}$ Sylow Theorem]

If $H$ is a $p$-subgroup of a finite group $G$, and $P$ is any Sylow $p$-subgroup of $G$, then there exists $x \in G$ such that $H < xPx^{-1}$. In particular, any two Sylow - $p$-subgroups of $G$ are conjugate.

Thm 2.32: ($3^{rd}$ Sylow Theorem)
If $G$ is a finite group and $p$ a prime, then the number of Sylow - $p$ - subgroups of $G$ divides $|G|$ and is of the form $kp+1$ for some $k \geq 0$.

## 2.4: Classification of Finite Groups

Prop 2.33: Let $p$ and $q$ be primes such that $p > q$. ~~If~~

(a) If $q \nmid p-1$, then every group of order $pq$ is isomorphic to the cyclic group $\mathbb{Z}_{pq}$.

(b) If $q \mid p-1$, then there are (up to $I^{sm}$) exactly two distinct groups of order $pq$: the cyclic group $\mathbb{Z}_{pq}$ and a non - abelian group $K$ generated by elements $c$ and $d$ such that

$$|c| = p, \quad |d| = q \quad dc = c^s d$$

where $s \not\equiv 1 \bmod p$ and $s^q \equiv 1 \bmod p$.

Corollary 2.34: If $p$ is an odd prime, then every group of order $2p$ is $\text{is}^{m}\text{c}$ either to the cyclic group $\mathbb{Z}_{2p}$ or the dihedral group $D_p$.

# 2.5: Nilpotent and Solvable Groups

Skip | Def$^n$ 2.35: Let $f: G \to G$ be an endomorphism of a group $G$. Then $f$ is said to be nilpotent if there exists a positive integer $n$ such that $f^n(g) = e$ for all $g \in G$.

Let $G$ be a group. The center $C(G) = \{a \in G \mid ax = xa \ \forall x \in G\}$ of $G$ is a normal subgroup. Let $C_2(G)$ be the inverse image of $C(G/C(G))$ under the cannonical projection

$$G \to G/C(G).$$ $C_2(G) \trianglelefteq G$ and $C_2(G) \supseteq C(G)$.

Continue this process by defining inductively: $C_1(G) = C(G)$ and $C_i(G)$ is the inverse image of $C(G/C_{i-1}(G))$ under the cannonical projection

$$G \to G/C_{i-1}(G).$$

Thus we obtain a sequence of normal subgroups of $G$, called the ascending central series of $G$:

$$\{e\} \leq C_1(G) < C_2(G) < \cdots$$

Def 2.35: A group $G$ is nilpotent if $C_n(G) = G$ for some $n$

EX 2.36: Every abelian group $G$ is nilpotent since $G = C(G) = C_1(G)$.

Thm 2.37: Every finite p-group is nilpotent.

Thm 3.38: The direct product of a finite no. of nilpotent groups is nilpotent.

Thm 3.39: If G is a finite abelian nilpotent group and m divides |G|, then G has a subgroup of order m.