Bézout's Wedderburn's theorem in arithmetic.
For Bézout's theorem in algebraic geometry

Nasr-allah Hitar
Anass Hajji

November 2022

Abstract

In mathematics, Bézout's identity (also called Bézout's lemma), named after Étienne Bézout, is the following theorem: Bézout's identity — Let a and b be integers with greatest common divisor d. Then there exist integers x and y such that ax + by = d. Moreover, the integers of the form az + bt are exactly the multiples of d.

1 Introduction

We will prove the theorem using some algebraic identities . also proving Wedderburn theorem .

Theorem 1 (Wedderburn theorem) *Wedderburn's little theorem states that every finite domain is a field. In other words, for finite rings, there is no distinction between domains, division rings and fields.*

let

$$(\mathbb{A}, +, \cdot)$$

a finite domain. let $a \in \mathbb{A} - 0_{\mathbb{A}}$ and let the application :

$$\phi_a : \mathbb{A} \longrightarrow \mathbb{A}$$

$$: x \longrightarrow a \cdot x$$

let x,y in $\mathbb{A}$ we have :

$$\phi_a(x) = \phi_a(y) \implies a \cdot x = a \cdot y$$

$$a \cdot (x - y) = 0 \implies x = y$$

so

$$(\forall a \in \mathbb{A} : \forall x, y \in \mathbb{A}) : \phi_a(x) = \phi_a(y) \implies x = y$$

so ϕ_a is an injective aplication
we have that :

$$Card(\mathbb{A}) = Card(\mathbb{A})$$

because $\mathbb{A}$ is finite. and (ϕ is an application from $\mathbb{A}$ to $\mathbb{A}$).
$\therefore \phi$ bijective .
so

$$\forall y \in \mathbb{A} : \exists! x \in \mathbb{A} : \phi_a(x) = y \therefore \forall x \in \mathbb{A} : \exists! y \in \mathbb{A} : a \cdot x = y$$

let $y = 1_{\mathbb{A}}$
$\therefore (\forall a \in \mathbb{A} : \exists! x \in \mathbb{A}) : a \cdot x = 1$
so every element $a \in \mathbb{A}$ had an inverse in the domain $(A, +, \cdot)$
$\therefore$ that every finite domain is a field.
and we knew that $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ (such that p is a prime) is a finite domain so : $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ is a finite field let n $\in \mathbb{Z}$: $(\forall p \in \mathbb{P})(\exists n^{-1} \in (\mathbb{Z}/p\mathbb{Z}))$:
$n \cdot n^{-1} \equiv 1[p]$
let m a positive integer such that gcd(n,m) = 1 , now if we took that prime p is a divisor of m we will find for all prime p exist in prime decomposition of m there exist a $n^{-1} \in \mathbb{Z}/p\mathbb{Z}$ such that : $n \cdot n^{-1} \equiv 1[p]$ for all p prime divisor of m , so using gauss theorem we will find that : $n \cdot \vartheta_n \equiv 1[M]$ such that ϑ_n is the product of all inverse by all prime divisors of m and :

$$M = \prod_{(p_i|m) \wedge (p_i \in \mathbb{P})} p_i$$

is the product of all primes divisors of m . then : let

$$\Phi = \prod_{(p_i|m) \wedge (p_i \in \mathbb{P})} \upsilon_{p_i}(m)$$

$$\therefore n \cdot n^{\Phi - 1} \cdot (\vartheta_n)^{\Phi} \equiv 1[M^{\Phi}] \tag{1}$$

it is trivial that :

$$m | M^{\Phi} \tag{2}$$

$\because \forall p_i \in \mathbb{P} : \nu_{p_i}(M^{\Phi}) > \nu_{p_i}(m)$
so by transitivity of $(\mathbb{Z}, |)$ we find that :

$$n \cdot \vartheta_n \equiv 1[m] \tag{3}$$

therefore : $\exists(\vartheta_n, u_m) \in \mathbb{Z}^2 : n\vartheta_n + mu_m = 1$
so bezout theorem because the other theorem is trivial.

2 references

1. W.K. Nicholson A SHORT PROOF OF THE WEDDERBURN-ARTIN THEOREM , NEW ZEALAND JOURNAL OF MATHEMATICS Volume 22 (1993), 83-86.
2. E. Artin, Zur Theorie der hypercomplexen Zahlen, Abh. Math. Sem. Univ. Hamburg 5 (1927), 251-260.
3. R. Brauer, On the nilpotency of the radical of a rinq, Bull. Amer. Math. Soc. 48 (1942), 752-758.
4. D.W. Henderson, A short proof of Wedderbum's theorem, Amer. Math. Monthly 72 (1965), 385-386.
5. J.H.M. Wedderburn, On hypercomple numbers, Proc. London Math. Soc. 6 (1908), 77-117.