Binomial Theorem

Let R be a commutative ring with $a, b \in R$.
For any $n \geq 0$ we have

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

$$\binom{n}{i} = \frac{n!}{i!\,(n-i)!}$$

Example

$$(a+b)^3 = \sum_{i=0}^{3} \binom{3}{i} a^i b^{3-i}$$

$$= \binom{3}{0} a^0 b^3 + \binom{3}{1} a b^2 + \binom{3}{2} a^2 b + \binom{3}{3} a^3 b^0$$

$$= b^3 + 3ab^2 + 3a^2 b + a^3$$

Show that the nilpotent elements of a commutative ring R form a subring

Let S be the set of nilpotent elements of R

1. $S \neq \emptyset$ because $0^1 = 0$ so $0 \in S$

2. Suppose $a, b \in S$

Then $a^n = 0$ and $b^m = 0$ for some $n, m \in \mathbb{Z}^+$

Let $d = n + m$

We claim that $(a-b)^d = 0$

We now show this.

By the binomial theorem we have

$$(a-b)^d = \sum_{i=0}^{d} a^i (-b)^{d-i} = \sum_{i=0}^{d} a^i (-1)^{d-i} b^{d-i}$$

If $i \geq n$ then $a^i = a^n a^{i-n} = 0 a^{i-n} = 0$

If $i < n$ then $d-i > m$ and we have

$$b^{d-i} = b^m b^{d-i-m} = 0 b^{d-i-m} = 0$$

This shows that $(a-b)^d = 0$ as claimed.

So $a-b \in S$

3 Suppose $a, b \in S$

Then $a^n = 0$, $b^m = 0$

for some $n, m \in \mathbb{Z}^+$

We have

$(ab)^n = a^n b^n$ (since R is commutative)

$= 0 b^n = 0$

so $ab \in S$

From 1, 2 and 3

S is a subring of R

Suppose R is a commutative ring without zero-divisors. Show that the characteristic of R is 0 or prime.

Note that we proved this in class when R has unity. Here we do not assume that R has unity.

Proof by contradiction:

Suppose that the characteristic of R is not

0 or prime. Then char $R = n$ where n is not prime, so $n = st$ where $0 < s < n$

$0 < t < n$

By the definition of the characteristic of R there exist $a, b \in R$ with

$s \cdot a \neq 0$ and $t \cdot b \neq 0$

Then $(s \cdot a)(t \cdot b) = (st) \cdot (ab)$

$= n \cdot (ab) = 0$

so R has a zero divisor a contradiction.

Let x and y belong to a commutative ring R with prime characteristic p

(a) Show that $(x+y)^p = x^p + y^p$

(b) Show that for all positive integers n $(x+y)^{p^n} = x^{p^n} + y^{p^n}$

(c) Find elements x and y in a ring of characteristic 4 such that $(x+y)^4 \neq x^4 + y^4$

(a) By the binomial theorem

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$$

Suppose $i \neq 0, p$

$$\binom{p}{i} = \frac{p!}{i!\,(p-i)!}$$

If $i \neq 0, p$ then both i and $p-i$ are less than p so $p \nmid i!$ and $p \nmid (p-i)!$

But $p \mid p!$.

Therefore p divides $\binom{p}{i}$

so $\binom{p}{i} x^i y^{p-i} = 0$ since char $R = p$

So $(x+y)^p = \binom{p}{0} x^0 y^p + \binom{p}{p} x^p y^0$

$$= y^p + x^p$$

(b) We prove this by induction on n.

<u>Base step</u> $n=1$

This is part a

Now let $n > 1$ and assume that the result is true for $n-1$

We have

$$(x+y)^{p^n} = \left((x+y)^{p^{n-1}}\right)^p$$

$$= \left(x^{p^{n-1}} + y^{p^{n-1}}\right)^p \quad \text{(by the induction hypothesis)}$$

$$= \left(x^{p^{n-1}}\right)^p + \left(y^{p^{n-1}}\right)^p \quad \text{(by the induction hypothesis)}$$

$$= x^{p^n} + y^{p^n}$$

(c) Let $R = \mathbb{Z}_4$

Then $\operatorname{char} R = 4$

Let $x = 1 \quad y = 1$

$$(x+y)^4 = (1+1)^4 = 2^4 = 0$$

$$x^4 + y^4 = 1^4 + 1^4 = 1 + 1 = 2$$

So $(x+y)^4 \neq x^4 + y^4$