survey of algebra hw 2

nxr8dq Sankalpa Banjade

September 2023

1 Introduction

Problems : 4.3.2(1,2), 4.3.4, 4.3.5(2) [you can assume any properties from (1)], 5.1.3, 6.1.3, 6.1.4, 6.3.1.

1)

Let R be a ring For a ∈ R and n ∈ the positive Reals define a^n inductively

Begin inductive proof have base cases. Base case

$a^n * a^1 = a^{n+1}$

Since the base case is true for m = 1, we must prove inductively that it will be true for all m >= 1. Lets let k be equal to some positive integer 1 and then plugging it in we have

$a^n * a^k = a^{m+k}$ (Due to Commutativity)

The above is true due to the property in the given that $a^{n+1} = a * a^n$

Now that it is true for some positive reals k lets prove it now for k + 1 to prove it for all positive integers.

$a^n * a^{k+1} = a^{n+k} * a^1$ Now since it is true for all positive reals k and since m and n have to be in the set of positive reals it proves this statement true for all m,n.

2 Part 2

2) Prove that $(a^n)^m = a^{n*m}$

We have two given cases when m = 1 that the equation just becomes

$(a^n)^m = a^n$ (Multiplicative Identity)

We also have a case for when m = 0 which makes the equation

$(a^n)^m = 1$

Since n * 0 = 0 (Already Proven in Class Zero Property of Multiplication) and any number to the power 0 is 1

Lets assume that P(n,k) holds true for some positive integer k

so that $(a^n)^k = a^{n*k}$ (Inductive Hypothesis)

Lets proceed with our indicative proof we will attempt to change k with k+1 so we can prove for any positive integer(Inductive step)

So we have

$(a^n)^(k+1) = a^{n*(k+1)}$
(Due to Commutativity)
From the given definition of exponentiation and from what we have already proven in exercises 1 we already know that when multiplying two numbers with the same base we can add their exponents. So the equation turns into.
$(a^n)^{(k+1)} = a^{(nk+n)}$
From Here we can factor out the n which comes from the Distributive Axiom. so left side side of the equation turns into, $(a^n)^k * a^n$
and the right side of the equation turns into $(a)^{n*(k+1)}$
So inductively since we have all ready proved the statement true for both when m either 0 or 1 and for any positive integer k, and now that we have also proved it true for k+1 then hence it is now prove the original statement for all positive integers.

3 4.3.4

Prove that for integers $1 <= k <= n$

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

This problem requires no induction as we can just compute the two sides as n pick k is equal to n-1 pick k added to n-1 pick k-1. The amount of times we can pick k objects from a set of n objects would be lets say that the n set is $a_1, a_2..., a_n$
Now without considering the last element a_n we would have a situation with n-1 pick k because we removed a single element from the set so we have n - 1 elements to pick from and choosing k
Now when we consider the collections that contain a_n since we already have picked an object a_n we have n-1 objects in the set again and since we are choosing "k" objects we have k-1 choices left due to already picking a_n. So now we have proved that n pick k is equal to the sum of n-1 pick k and n-1 pick k-1, as the two cases for which the combination do or do not contain the element a_n works for every elemenet in the set of n objects.

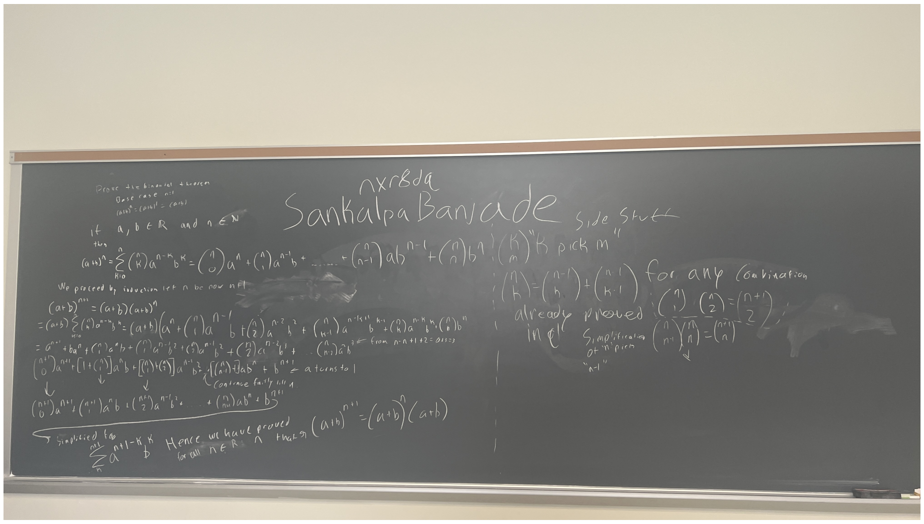
4 4

Prove the *binomial theorem*: if $a, b \in R$ and $n \in N$ then

(2) Prove the *binomial theorem*: if $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$, then

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \cdots + \binom{n}{n-1} ab^{n-1} + \binom{n}{n} b^n.$$

(In fact, this holds with $\mathbb{R}$ replaced by any commutative ring R, provided we interpret the terms in this sum as in Exercise 4.3.5 below).



5 5

4.3.5(2) Prove that R has finitely many elements, then for any a $\in R$ there is some k > 0 such that ka $= 0$. Given:
0a $= 0$
$(n+1)a = na + a$ If n < 0, then we define na = -((-n)a).
We begin by contradiction, that there is an element a in the ring R such that for any a $\in R$ that in the set of Z_+ that ka $\neq 0$. We make a set such that every element is a multiple of the element a, S $= a, 2a, 3a, 4a, 5a.....$ we know that every element is non zero and non negative due to the restrictions we put in the beginning. Since we know that R has non infinite elements (since there is not infinite numbers) we know that there exists an element m that is the largest positive integer in S that is multiplied with a. So the set S now becomes S $= a, 2a, 3a, 4a, 5a..., ma$ and we know that in the set S that, elements a through (m-1) * a are distinct, however we know that ma = na for some n that is less than m and in the set S we know that (m-1) * a can't equal any other element in S due to them being all distinct from each other, therefore we consider (m-1) * a as not in the set hence we arrive at a contradiction making ka $\neq 0$ false . That there does exist an element k such that ka $= 0$.

6 6

5.1.3 If n $\in$ the set of positive integers then n >= 1 (In other words there are no integers strictly between 0 and 1. *Hint* Consider the set $S = n \in Z_+ : 0 < n < 1$ You want to show that S = the empty set, so suppose towards contradiction that S does not equal the empty set. By the well ordering principal it follows

that there is a minimal element $n \in S$ Can you derive a contradiction from this? We will begin with the well ordering principle, the well ordering principles tell us that there must exists at least one element we will call that element a. If it does indeed exist we must assume that it is between 0 and 1. Which gives us this inequality $0 < a < 1$ we can then multiply this entire inequality by a.
0 * a = 0 (Zero Property)
a * a = a^2
1 * a = a
We have arrived at a contradiction because if a was indeed a positive integer than a^2 would have to be greater than a hence we have proved by contradiction that there exists no integers between 0 and 1.

7 7

6.1.3 Prove ($\delta 4$) and ($\delta 5$)

If $a|b$ then $a|bc$ for all c $\in Z$

The definition of a divisor
b = a * k for some k $\in Z$
we multiply both sides by c

b * c = (a*k) * c
We utilise the commutative property of multiplication

b * c = c * (a*k)
We assume that there is closure under multiplication so if bc $\in Z$ then $b, c \in Z$ so we now have reached our definition of a divisor. So now by definition we can state that $a|bc$.

Prove $\delta 5$
ie if $a|b$ and $b|c$ then $a|c$ (transitive property)

b = a * k for some k $\in Z$
well set this value b time a constant p $\in Z$ equal to c c = b * p
by definition of a divisor for p $\in Z$

we now substitute back what we had for b in the original equation
c = (a*k) * p by substitution
we now utilise the commutative property of multiplication
c = p * (a*k)
Once again we assume that there is closure under multiplication so if kp $\in Z$ then $k, p \in Z$ so we now have reached our definition of a divisor. So now by definition we can state that $a|c$.

8 8

6.1.4 Given $a, b, c \in Z$ with $a|bc$, must it be the case that $a|b$ or $a|c$. If this is always true, prove it. Otherwise find a counter example.
This statement is not true, as a counter example would be when a = 15, b = 25 and c = 9 15 does not divide 25 nor does it divides 225 the product of b and c as 15 squared is 225.

9 9

6.3.1 Let a, b, q, r be integers satisfying the equation $a = bq+r$ Then the gcd(a,b) = gcd(b,r) Giving us the following algorithm with integers a and b fixed, and we assume that both a and b are $\in Z_+$ and without loss of generality that we have $a >= b$ we can proceed with long division that we may divide a with b getting a remainder that satisfies $a = bq + r//$

with $q, r \in Z$ and $0 <= r < b$ // Proof: we will call the gcd(a,b) equal to d meaning that a = dv and that b = du for some $u, v \in Z$

We have that
a = bq + r (Given)
a- bq = r (By subtracting r from both sides) apply substitution a -(du)q = r apply substitution again (dv) - (du)q = r We utilise the converse of the distributive property and the distributive property itself to properly factor out the d on the left hand side of the equation d(v-uq) = r with this we have shown that r is a product between d and an integer and by definition of divisor we have that $d|r$, Now utilising the transitive property we have that d not only divides r but also a and b as well. Meaning that the gcd of a and b is equal to the gcd of b and r.