

MAS 117

Introduction to Algebra

Solutions 7

March 2007

- 1 (a) n is never equal to $n + 1$. In describing the inductive step, you should say either

Assume that $A(n)$ holds; we have to prove that $A(n + 1)$ holds.

or

Assume the statement is true for $n = k$; we have to prove that it is true for $n = k + 1$.

- (b) There are two misunderstandings here, as well as some very clumsy writing. This student may understand the notion “one-to-one”, but hasn’t expressed it well. Every function $F : A \rightarrow B$ gives a unique output in B for each input in A ; one-to-one means that different inputs produce different outputs, i.e. $a_1 \neq a_2$ implies $F(a_1) \neq F(a_2)$. The student also seems to think that “onto” is the negation of “one-to-one”.

- (c) There are several misunderstandings here. First, the student seems to think that the contrapositive of “if A , then B ” is “if not- A , then not- B ”. It should be “if not- B , then not- A ”.

Second, the two statements have been negated incorrectly. The negation of “an even integer greater than 2” isn’t “an odd integer less than 2”. You could write it as “an odd integer, or an integer less than or equal to 2, or anything which isn’t an integer”. Better, surely, to say “not an even integer greater than 2”. And the negation of “the sum of two prime numbers” isn’t “the sum of two non-prime numbers”, but “not the sum of two prime numbers”.

So the correct answer is

“If n is not the sum of two prime numbers, then n is not an even integer greater than 2.”

- (d) Sorry – I got confused here! The word “distributive” should have been “associative”, and the answer I had in mind was

Union is confused with intersection, and the associative law is confused with the commutative law. To verify the claim, we must show that $(A \cup B) \cup C = A \cup (B \cup C)$.

Of course, there are two distributive laws, namely

$$(A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \text{ and } (A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$

and neither of them just involves union. So an answer along the lines “the commutative law is confused with the distributive law” would suffice.

2 If $x^3 + x + 1$ is reducible, it must be a product of factors of degrees 1 and 2. The factor of degree 1 would have to be either x or $x + 1$ (the only polynomials of degree 1), and so either 0 or 1 would be a root of $x^3 + x + 1 = 0$. But in $\mathbb{Z}_2$ we have

$$0^3 + 0 + 1 = 1^3 + 1 + 1 = 1.$$

A field K of order 8 can now be constructed as the set of all elements $u + va + wa^2$, where $u, v, w \in \mathbb{Z}_2$ and a is an element satisfying $a^3 + a + 1 = 0$. Notice that since $-1 = 1$, we have $-x = x$ for all $x \in K$. So we have

$$a^3 = a + 1, \quad a^4 = a^2 + a,$$

and so we can multiply any two elements of the form $u + va + wa^2$ and reduce the result to the same form. The tables are

+	0	1	a	$1+a$	a^2	$1+a^2$	$a+a^2$	$1+a+a^2$
0	0	1	a	$1+a$	a^2	$1+a^2$	$a+a^2$	$1+a+a^2$
1	1	0	$1+a$	a	$1+a^2$	a^2	$1+a+a^2$	$a+a^2$
a	a	$1+a$	0	1	$a+a^2$	$1+a+a^2$	a^2	$1+a^2$
$1+a$	$1+a$	a	1	0	$1+a+a^2$	$a+a^2$	$1+a^2$	a^2
a^2	a^2	$1+a^2$	$a+a^2$	$1+a+a^2$	0	1	a	$1+a$
$1+a^2$	$1+a^2$	a^2	$1+a+a^2$	$a+a^2$	1	0	$1+a$	a
$a+a^2$	$a+a^2$	$1+a+a^2$	a^2	$1+a^2$	a	$1+a$	0	1
$1+a+a^2$	$1+a+a^2$	$a+a^2$	$1+a^2$	a^2	$1+a$	a	1	0

and

·	0	1	a	$1+a$	a^2	$1+a^2$	$a+a^2$	$1+a+a^2$
0	0	0	0	0	0	0	0	0
1	0	1	a	$1+a$	a^2	$1+a^2$	$a+a^2$	$1+a+a^2$
a	0	a	a^2	$a+a^2$	$1+a$	1	$1+a+a^2$	$1+a^2$
$1+a$	0	$1+a$	$a+a^2$	$1+a^2$	$1+a+a^2$	a^2	1	a
a^2	0	a^2	$1+a$	$1+a+a^2$	$a+a^2$	a	$1+a^2$	1
$1+a^2$	0	$1+a^2$	1	a^2	a	$1+a+a^2$	$1+a$	$a+a^2$
$a+a^2$	0	$a+a^2$	$1+a+a^2$	1	$1+a^2$	$1+a$	a	a^2
$1+a+a^2$	0	$1+a+a^2$	$1+a^2$	a	1	$a+a^2$	a^2	$1+a$