February 17, 2018

Name:

Test 1, Math 5330

You have **90** minutes to complete the test. You cannot use any books or notes.

1. State the Well-Ordering Principle for the set of natural numbers.Answer: Every non-empty subset of natural numbers has a minimum.

2. Deduce from the Well-Ordering Principle the Principle of Mathematical Induction. Answer: Let S be a non-empty subset of natural numbers and assume $1 \in S$ and whenever $k \in S$ then $k+1 \in S$. We need to show $S = N$. Assume $T = N \backslash S$ is non-empty. Then T is a non-empty set of natural numbers and therefore has a smallest element k. We cannot have $k = 1$ because $1 \in S$. Therefore k has a predecessor $k-1 < k$. Because k is the smallest number not in S, it must be the case that $k-1 \in S$. But then $k \in S$. We have reached a contradiction. Thus $T = \emptyset$, which is $S = N$.

3. State Mathematical Induction, second form, and prove that every number $n > 1$which is not prime is a product of prime numbers. Answer: Let $P(n)$ be a statement about positive numbers. Assume that i) $P(1)$ is true and ii) that $P(m)$ is true in case that for all $k < m$ one has that $P(k)$ is true. Then $P(n)$ is true for all n. The second form works where there is no easy way to go from k to $k+1$. For example assume that n is a natural number where every natural number $k < n$ is a product of primes. If n is not a prime then it is a product $a \cdot b$ of two smaller numbers. If we assume that $a = p_1 \cdot \ldots \cdot p_s$ and $b = q_1 \cdot \cdots q_t$ are products of primes, then $n = a \cdot b = p_1 \cdot \ldots \cdot p_s \cdot q_1 \cdot \cdots q_t$ is a product of primes.

4. State the definition of a group. Give an example of a commutative and of a non-commutative group. Answer: A group is a set G with a binary operation $*$ which is associative, that is $(a * b) * c = (a * (b * c)$, there is unit e such that $a * e = e * a = a$ and every element a has an inverse a^{-1} such that $a * a^{-1} = a^{-1} * a = e$. A group is commutative if $a * b = b * a$ holds for all a and b in G. The integers with addition form a commutative group. invertible 2×2 –matrices form a non-commutative group.

5. Let $A = \{a, b, c\}$ be a three element set. Define operations $*, {}^{-1}, e$ on A which makes $(A, *, {}^{-1}, e)$ a group. Answer: Integers modulo 3 form with respect to addition modulo 3 a group with three elements. You may identify a with $0, b$ with 1 and c with 2. Then $b + c = a = 0$ and $-b = c, -c = a$.

6. Let $(G, *, {}^{-1}, e)$ be a group. Show that the group is abelian iff $(a * b)^2 = a^2 * b^2$. Answer: This was a homework problem:
$(a * b)^2 = (a * b) * (a * b) = a * (b * a) * b, (a * b)^2 = a^2 * b^2 = a * (a * b) * b$ by assumption. Thus $a * (b * a) * b = a * (a * b) * b$ and we get $a * b = b * a$ by cancellation.

7. Define the additive group $(\mathsf{Z}_n, \oplus)$ of integers modulo n. You have to state exactly what its elements are, how $\oplus$ is defined, what the identity is, and how the inverse of an element is defined. Answer: $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ has n –elements. Actually 0 stands for all multiples of n, that is for $n\mathbb{Z}, 1$ stands for $1 + n\mathbb{Z}$, *etc* Addition is modulo n. The identity is

$n\mathbb{Z}$ and $-k$ stands for $-k + n\mathbb{Z}$.

8. **a**. Find the additive inverse of 49 modulo 50. Answer: $-49 = 49 + 50 = 1,$ indeed $49 + 1 = 50 = 0 \bmod 50$

b. Solve $20 + x = 7$ modulo 50. You need to give an x between 0 and 49. Answer: $x = -20 + 7 = -13 = -13 + 50 = 37$ modulo 50

9. Let $(G, *, ^{-1}, e)$ be a group. Prove that for given g and h the equation $g * x = h$ has a unique solution x. Answer: Multiplication of both sides by g^{-1} yields $g^{-1} * (g * x) = g^{-1} * h$ which yields $x = g^{-1} * h$. This gives uniqueness. Existence is $g * (g^{-1} * h) = h$. We needed associativity

10. Let $(G, *, ^{-1}, e)$ be a group and let $x, y, z \in G$. Prove the cancellation laws:

a. If $x * y = x * z,$ then $y = z$. Answer: Multiply both sides by x^{-1} from the left: $x^{-1} * (x * y) = x^{-1} * (x * z), (x^{-1} * x) * y = (x^{-1} * x) * z, y = z$ Associativity was used.

b. If $y * x = z * x,$ then $y = z$. Answer: similar as a.