MTH 4441 – Definitions, Theorems, and Proofs to Know for Test #1

Fall 2017

Pat Rossi Name _____

Part #1 Definitions

1. Define **congruent (congruence) modulo** n.

   Let $n \geq 2$ be a natural number. Then integers x and y are **congruent modulo** n, denoted $x \equiv y \pmod{n}$, exactly when $x - y = kn$, for some integer k. (i.e., $x \equiv y \pmod{n}$ exactly when $x - y$ is a multiple of n.)

2. **(Alternative Definition)** Define **congruent (congruence) modulo** n.

   Let $n \geq 2$ be a natural number. Then integers x and y are **congruent modulo** n, denoted $x \equiv y \pmod{n}$, exactly when x and y have the same "proper remainder" (i.e., $r \in \{0, 1, 2, \ldots, n-1\}$) when divided by n.

3. Define **group.**

   Let G be a set and let $*$ be a binary operation defined on the elements of G. Then $(G, *)$ is a group exactly when the following conditions hold:

   i. G is **closed** under $*$. (i.e. $x * y \in G$, $\forall x, y \in G$)

   ii. $*$ is **associative.** (i.e. $(x * y) * z = x * (y * z)$, $\forall x, y, z \in G$)

   iii. G has an identity element e. (i.e., $\exists\ e \in G$ such that $x * e = e * x$, $\forall x \in G$.)

   iv. Each element $x \in G$ has an inverse x^{-1}, such that $x * x^{-1} = e = x^{-1} * x$

4. Define **subgroup.**

   Let $(G, *)$ be a group and let $H \subseteq G$. Then $(H, *)$ is a **subgroup** of $(G, *)$, denoted $H \leq G$, exactly when $(H, *)$ is a group.

5. Define the **order of a group.**

   Suppose that the total number of elements of $(G, *)$ is $n \in \mathbb{N}$. Then $(G, *)$ is a **finite group** of **order** n, denoted $|G| = n$.

   Otherwise, $(G, *)$ is an **infinite group.**

6. Define **cyclic subgroup.**

   Let $a \in (G, *)$. The **cyclic subgroup** generated by a, denoted $\langle a \rangle$, is the smallest subgroup of $(G, *)$ that contains both a and a^{-1}.

   If $(H, *)$ is a cyclic subgroup of $(G, *)$, generated by a, then we write $(H, *) = \langle a \rangle$.

   If $(G, *) = \langle a \rangle$, then we say that $(G, *)$ is a **cyclic group** generated by a

7. Define **Cartesian product.**

   Given sets A and B, the **Cartesian product** of A and B (or **"the product"** of A and B), denoted $A \times B$, is defined as:

   $$A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$$

   Similarly, given sets A, B, and C, the **Cartesian product** of A, B, and C (or **"the product"** of A, B, and C), denoted $A \times B \times C$, is defined as:

   $$A \times B \times C = \{(a, b, c) : a \in A,\ b \in B,\ \text{and } c \in C\}$$

8. Define **identity.**

   Given a group $(G, *)$, the **identity element** (or **identity**) is the unique element $e \in (G, *)$ having the property that:

   $$e * x = x \quad \text{and} \quad x * e = x, \quad \forall x \in G.$$

9. Define **inverse.**

   Given a group $(G, *)$ and an element $x \in (G, *)$, the **inverse** of x, denoted x^{-1}, is the unique element having the property that:

   $$x * x^{-1} = e \quad \text{and} \quad x^{-1} * x = e.$$

10. Define **Commutative.**

    Given a binary operator $*$ on a non-empty set G, the operator $*$ is **commutative** if:

    $$x * y = y * x \quad \forall x, y \in G.$$

11. Define **Associative.**

    Given a binary operator $*$ on a non-empty set G, the operator $*$ is **associative** if:

    $$(x * y) * z = x * (y * z) \quad \forall x, y, z \in G.$$

12. Define **Abelian Group.**

    A group $(G, *)$ is **abelian** if the operator $*$ is commutative.

13. Define **closure, closed.**

    A binary operator $*$ is **closed** on a set G, if $x * y \in G$, $\forall x, y \in G$.

14. Define **one-to-one**

    A function $f : X \to Y$ is **one-to-one** if no two elements in X get assigned to the same element of Y by the function f.

    (i.e., A function $f : X \to Y$ is **one-to-one** if, for $x_1, x_2 \in X$, with $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$.)

15. Define **onto**

    A function $f : X \to Y$ is **onto** if, given $y \in Y$, $\exists\ x \in X$ such that $f(x) = y$.

16. Define **isomorphism, isomorphic**

A function $\phi : (G_1, *_1) \to (G_2, *_2)$ is an **isomorphism** if:

(a) $\phi : G_1 \to G_2$ is one-to-one and onto

and

(b) $\phi(a *_1 b) = \phi(a) *_2 \phi(b)$, $\forall a, b \in G_1$

If such an isomorphism exists, then $(G_1, *_1)$ and $(G_2, *_2)$ are said to be **isomorphic.**

Part #2 Theorems

17. **Thm A -** list properties that are preserved by an isomorphism $\phi : (G_1, *_1) \to (G_2, *_2)$

(a) **Cardinality -** (Isomorphic groups have the "same number of elements")

1. If G_1 is finite and contains n elements, then G_1 is finite and contains n elements.
2. If G_1 is countably (denumerably) infinite, then G_2 is countably (denumerably) infinite.
3. If G_1 is uncountably (non-denumerably) infinite, then G_2 is uncountably (non-denumerably) infinite.

(b) **Identities**

1. If e_1 is the identity of $(G_1, *_1)$, then e_2 is the identity of $(G_2, *_2)$

(c) **Inverses**

1. If x^{-1} is the inverse of x in $(G_1, *_1)$, then $\phi\left(x^{-1}\right)$ is the inverse of $\phi(x)$ in $(G_2, *_2)$

(d) **Commutativity -** if $(G_1, *_1)$ is commutative (abelian), then $(G_2, *_2)$ is commutative (abelian)

(e) **Cyclic Groups and generators**

1. If $(G_1, *_1)$ is cyclic with generator a, then $(G_2, *_2)$ is cyclic with generator $\phi(a)$

(f) **Subgroups**

1. If $(H, *_1) \leq (G_1, *_1)$, then $(\phi(H), *_2) \leq (G_2, *_2)$
2. If $(H, *_1)$ is a **cyclic subgroup** of $(G_1, *_1)$, of order k and having generator a; then $(\phi(H), *_2)$ is a **cyclic subgroup** of $(G_2, *_2)$, of order k and having generator $\phi(a)$

(g) **Number and Order of Subgroups**

1. If $(G_1, *_1)$ has k subgroups of order n, then $(G_2, *_2)$ has k subgroups of order n

18. **Thm B -** Identities and Inverses

    (a) The **identity** of a group **is unique**

    (b) The **inverse** of an element x **is unique**

    (c) The inverse of a product is the product of the inverses, **in reverse order**

    (i.e., $(ab)^{-1} = b^{-1}a^{-1}$

19. **Thm C-** In a group, the **Cancellation Laws** hold

    (i.e., $xa = xb \Rightarrow a = b$ and $ax = bx \Rightarrow a = b$, $\forall a, b, x \in G$)

Cyclic Groups In General

20. **Thm 1** - every subgroup of a cyclic group is cyclic

21. **Thm 2** - Any two finite cyclic groups of order n are isomorphic (i.e., Any two finite cyclic groups of the same order are isomorphic.)

22. **Thm 3 -** An isomorphism ϕ between two finite cyclic groups of order n is completely defined by the value of $\phi(a)$, where a is a generator (*any* generator) of the first group. Since isomorphisms map "generator to generator," $\phi(a)$ must be a generator (*any* generator) of the second group. The value of $\phi(b)$ for any element b of the first group is completely determined by the value of $\phi(a)$.

23. **Thm 4 -** The property of two groups being isomorphic is an equivalence relationship. That is to say:

    (a) $(G, *) \cong (G, *)$

    (b) $(G, *_1) \cong (H, *_2) \Rightarrow (H, *_2) \cong (G, *_1)$

    (c) If $(G, *_1) \cong (H, *_2)$ and $(H, *_2) \cong (K, *_3)$, then $(G, *_1) \cong (K, *_3)$

Cyclic Groups With "Additive Notation"

24. **Thm 5 -** The generators of the cyclic group $(\mathbb{Z}_n, +)$ are exactly those non-zero "proper remainders" $\{1, 2, 3, \ldots, n-1\}$ that are relatively prime to n.

25. **Thm 6 -** Given the cyclic group $(\mathbb{Z}_n, +)$, if $a \in \{1, 2, 3, \ldots, n-1\}$, then a generates a cyclic subgroup of order $\frac{|G|}{d}$ where $d = \gcd(a, n)$.

Cyclic Groups With "Multiplicative Notation"

26. **Thm 7 -** $k \in U_n$ is a generator of $(U_n, \cdot)$ exactly when n is the least positive integer such that $k^{n-1} \equiv 1 \bmod n$

27. **Cor** - $k \in U_n$ is a generator of $(U_n, \cdot)$ exactly when n is the least positive integer such that $k^{\frac{n-1}{2}} \equiv n - 1 \bmod n$

28. **Thm 8 -** Let $(G, *) = \langle a \rangle$ be a finite cyclic group of order n. Then a^m is a generator of G exactly when m and n are relatively prime. (i.e., exactly when $\gcd(m, n) = 1$).

29. **Thm 9** - If G is cyclic with generator a, and $H < G$, then either:

    (a) $H = \langle e \rangle$ (i.e., $H = (\{e\}, *)$

    or

    (b) $H = \left\langle a^k \right\rangle$, where k is the least natural number such that $a^k \in H$.

30. **Thm 10 -** Let $G = \langle a \rangle$ be a *finite* cyclic group of order n. For any integer m, $\langle a^m \rangle = \left\langle a^d \right\rangle$, where $d = \gcd(m, n)$.

31. **Thm 11 -** Suppose that G is a finite cyclic group of order n. Then:

    (a) for any generator $a \in G$, n is the least natural number such that $a^n = e$.

    and

    (b) if $a^s = a^t$, then $s \equiv t \bmod n$

Part #3 Some Proofs That We Should Know

32. Prove that the identity of a group $(G, *)$ is unique. (Do NOT appeal to the cancellation laws.)

    Remark: We will show that the identity element is unique by assuming that there are (at least) **two** identity elements in the group and showing that they must be one, and the same, element.

    pf/ Suppose that there are two identity elements, e and e_1 in G.

    Observe: $e = e * e_1$ (because e_1 is an identity)

    Also: $e * e_1 = e_1$ (because e is an identity)

    $\Rightarrow e = e * e_1 = e_1$

    i.e., $e = e_1$ ■

33. Prove that the inverse of an element x in a group $(G, *)$ is unique. (Do NOT appeal to the cancellation laws.)

    Remark: We will show that an element x has a unique inverse by assuming that x has (at least) two inverses elements in the group and showing that they must be one, and the same element.

    pf/ Suppose that x has (at least) two inverses, y and z in G.

    Then $xy = e$ and $yx = e$ (because y is an inverse of x)

    Also: $xz = e$ and $zx = e$ (because z is an inverse of x)

    Observe: $y = ye = y(xz) = (yx)z = ez = z$

    i.e., $y = z$ ■