Math 3520 - Test 2 Review

1 Number Theory

1. Let $a, b, c, d \in \mathbb{Z}$ with $b \neq 0$. Show if $a|b$ and $b|c$ then $a|c$.
2. Let $a, b, c, x, y \in \mathbb{Z}$. Show if $a|b$ and $a|c$ then $a|ax + by$.
3. Let $a, b, c, d \in \mathbb{Z}$ with $c \neq 0$. Show if $a|b$ and $c|d$ then $ac|ad + bc$.
4. Prove $3|n^3 - n$ for every integer n.
5. Let $a, b, c \in \mathbb{Z}$. If $a|bc$ and $\gcd(a, b) = 1$ then $a|c$.
6. Let $a, b \in \mathbb{Z}$ and let p be a prime. If $p|ab$ then $p|a$ or $p|b$.
7. Let $a, b, c \in \mathbb{Z}$ where $\gcd(a, b) = 1$. If $a|c$ and $b|c$ then $ab|c$.
8. Let $n \in \mathbb{Z}$ be odd. Prove $n^2 \equiv 1 \mod 4$.
9. Let $n \in \mathbb{Z}$ be odd. Prove $n^2 \equiv 1 \mod 8$.
10. Let $a, b, c \in \mathbb{Z}$ so that $a^2 + b^2 = c^2$. Prove $4|ab$ (hint use 9).
11. Prove or disprove if $a, b \in \mathbb{Z}$ and a, b are odd then $8|a^2 - b^2$.
12. Prove $\sqrt{3}$ is irrational.
13. For the following pairs of numbers, find their gcd and and find a linear combination of the numbers equal to their gcd.
    (a) $a = 78$ and $b = 48$
    (b) $a = 79$ and $b = 49$
    (c) $a = 253$ and $b = 207$

2 Group Theory

14. State the definition of an **Algebraic sturcture** and a **binary operation**.
15. State the definition of a **group**.
16. State the definition of an **Abelian group**.

17. State and prove the cancellation law.

18. Are the following algebraic structures groups? If it is a group prove it. If not prove it is not a group.

    (a) $(\mathbb{Q}^*, \cdot)$ where $\cdot$ is regular multiplication.

    (b) $(\mathbb{Z}, \odot)$ where $a \odot b = a + b - 2$.

    (c) $(\mathbb{Z}, \circledast)$ where $a \circledast b = ab + a + b$.

    (d) $(\mathbb{Q} \setminus \{-1\}, \circledast)$ where $a \circledast b = ab + a + b$.

19. For the following algebraic structures write the operation tables. State if the structure is a group or not. If not state which property fails and how. Identify the identity in each case.

    (a) $(\mathbb{Z}_5, +)$

    (b) $(\mathbb{Z}_5, \cdot)$

    (c) $(\mathbb{Z}_6^*, \cdot)$

    (d) $(S_3, \circ)$

    (e) $(D, \circ)$ where

$$D = \{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$$

    (f) $(D, \circ)$ where $D \subseteq S_3$ defined as

$$D = \{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$$

    (g) $(M, \cdot)$ where $M \subseteq GL_2(\mathbb{R})$ defined as

$$M = \{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\}$$

20. We showed in class that some groups are "the same" by finding a function from one group to the other that preserved the operation. The following pairs of groups are "the same" in that sense find the function and verify that it preserves the operation.

    (a) $(Z_4, +)$ and $(Z_5^*, \cdot)$

(b) $(Z_2, +)$ and $(M, \cdot)$ where $M \subseteq GL_2(\mathbb{R})$ defined as

$$M = \{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\}$$

(c) $(Z_{12}^*, \cdot)$ and $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$

21. Let G be a group prove

    (a) The identity in G is unique.

    (b) If $a \in G$ then a^{-1} is unique.

    (c) If $a \in G$ then $(a^{-1})^{-1} = a$.

    (d) If $a, b \in G$ then $(ab)^{-1} = b^{-1}a^{-1}$.

22. Let G be a group prove and let $a, b \in G$. If a and b commute then a^{-1} and b^{-1} commute.

23. Let $(G, *)$ be a group prove and let $a, b, c \in G$. Prove the following equations have an unique solution $x \in G$.

    - $a * x * c = b$
    - $c * a * x = b$

24. Let $(G, *)$ be a group prove.
    Assume there is some element $f \in G$ so that for some elemnt $a \in G$ we have $af = a$. Is f the identity? Prove or disprove.

25. Let $(G, *)$ be a group prove.
    If $a * a = e$ for all $a \in G$ then G is Abelian.

3 More Group Theory

26. Definition of a **subgroup** and of an **isomorphism**.

27. For the group $(\mathbb{Z}, +)$ prove, using the 2-step subspace test, that $H = \{3n : n \in \mathbb{Z}\}$ is a subgroup.

28. For the group $(\mathbb{Z}, +)$ Show $H = \{2n + 1 : n \in \mathbb{Z}\}$ is not a subgroup.

29. For the group $(S_3, \circ)$ Show

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

is not a subgroup of S_3.

30. Let G be any group and let g be a fixed element of G then prove, using the 2-step subspace test, that $H = \{gag^{-1} | a \in G\}$ is a subgroup.

31. Let G be any group then prove, using the 2-step subspace test, that $H = \{a \in G | ag = ga \, \forall g \in G\}$ is a subgroup.

32. For the groups $G_1 = (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, +)$ and $G_2 = (\mathbb{Z}_8, +)$

    (a) Find the orders of the elements $(1, 1, 1)$ and $(1, 0, 1)$ in G_1 and the orders of the elements 1, 2, 3 in G_2?

    (b) Are any of the above elements generators for their respective groups?

    (c) Why aren't the groups isomorphic?

33. For the groups $G_1 = (\mathbb{Z}_9^*, +)$ and $G_2 = (Z_6, +)$

    (a) Find the orders of three diffferent non identity elements in G_1 and the orders of the elements 1, 2, 3 in G_2?

    (b) Are any of the above elements generators for their respective groups?

    (c) The two groups are isomorphic. Find the isomorphism $f : G_1 \to G_2$.

34. Note that $(G, \cdot)$ is a group where $G = \{2^n : n \in \mathbb{Z}\}$ and $\cdot$ is regular multiplication. Prove Axioms G_1 and G_3 for $(G, \cdot)$.

35. Note that $(G, \cdot)$ is a group where $G = \{2^n : n \in \mathbb{Z}\}$ and $\cdot$ is regular multiplication. Show $G \cong \mathbb{Z}$ where $\mathbb{Z}$ is a group over addition. I used the isomorphism $f : \mathbb{Z} \to G$. We need to prove f preserves the operation and that f is a bijection.