Math 322 **Fall 2008** **Exam 3 review**

Definitions: Group homomorphism, isomorphism; kernel of a group homomorphism; Cayley map; subgroup generated by a subset; commutator; commutator subgroup; partition of a set; direct product; relation on a set; antisymmetric, reflexive, transitive and symmetric relations; partial ordering, poset; least/greatest element of a poset; n-ary operation; associative and commutative operation; identity; inverse; semigroup; monoid; conjugate; conjugacy class; ring; commutative ring; unital ring; unit; subring; group of units; ring homomorphism, isomorphism; kernel of a ring homomorphism; right ideal; left ideal; ideal; coset of an ideal; quotient ring; principal ideal; Euler totient (ϕ-function); zero divisor; integral domain; characteristic of an integral domain; division ring; field; subfield; field extension; prime subfield; field of fractions; algebraic, transcendental over R; degree of a polynomial; leading coefficient; monic polynomial; reducible/irreducible polynomial; associates; prime; root of a polynomial; multiplicity of a root; greatest common divisor of polynomials; relatively prime; simple extension (of fields); minimal polynomial; splitting field.

1. Let $G = \langle g \rangle$ be a cyclic group of order 6, and let $\varphi : G \to G$ be the map $\varphi(x) = x^4$ for all $x \in G$.

a. List the elements of the image $\varphi(G)$.

b. List the elements of the preimage $\varphi^{-1}(g^2)$.

2. Let $G = \langle (1324) \rangle \leq S_4$. Define a map $\varphi : \mathbb{Z}_4 \to G$ by setting $\varphi(\bar{a}) = (1324)^a$ for $\bar{a} \in \mathbb{Z}_4$. Prove that φ is an isomorphism.

3. Let N be a normal subgroup of G, and let $\pi : G \to G/N$ be the natural map $\pi(g) = \bar{g} = gN$. Prove that the order of $\bar{g}$ divides the order of g.

4. Let G be a cyclic group of order 12.

a. Let $s \in \mathbb{N}$. Prove that the map $\varphi_s : G \to G$ defined by $\varphi_s(g) = g^s$ is a homomorphism.

b. Explain why φ_s is an isomorphism if and only if s is relatively prime to 12 (that is, $\gcd(s, 12) = 1$).

5. Let $Q = \{1, -1, i, -i, j, -j, k, -k\}$ be the quaternion group. By Lagrange's Theorem, any subgroup of Q has order 1, 2, 4, or 8.

a. Why is every subgroup of order 8 normal?

b. Why is every subgroup of order 4 normal?

c. Why is every subgroup of order 1 normal?

d. What is the center of Q? Justify (*i.e.*, prove) your answer.

6.a. Let G be a group and let g_1 and g_2 be elements of G. Define the commutator $[g_1, g_2]$ of g_1 and g_2.

b. Let $H = [G, G]$ be the commutator subgroup of G. Prove that G/H is abelian.

7. Let $G = \langle g \rangle$ be a cyclic group of order 6, and let $\varphi : G \to G$ be the map $\varphi(x) = x^4$ for all $x \in G$.

a. List the elements of the image $\varphi(G)$.

b. List the elements of the preimage $\varphi^{-1}(g^3)$.

8. Let G be an abelian group. Show that the map $\iota : G \to G$ defined by $\iota(g) = g^{-1}$ (for all $g \in G$) is a homomorphism.

9.a. Give an example of a homomorphism $\varphi : G \to H$ such that the image $\varphi(G)$ is not a normal subgroup of H.

b. Suppose G is an abelian group. Prove that the image $\varphi(G) \leq H$ is abelian.

10.a. Let G and H be groups. Define the direct product $G \times H$. That is, define $G \times H$ as a set, and describe the group operation.

b. Prove that $\mathbb{Z}_2 \times \mathbb{Z}_5 \cong \mathbb{Z}_{10}$ by finding an explicit map and proving that it is an isomorphism.

11.a. Let G be a group and let g_1 and g_2 be elements of G. Define the commutator $[g_1, g_2]$ of g_1 and g_2.

b. Compute the following commutators in S_4: $[(12), (13)]$, $[(1234), (12)]$, $[(142), (134)]$.

12. Let G be a group of order pq, where p and q are distinct positive primes, and let $g \in G$.

a. What are the possible orders of g? Why?

b. Suppose G is *not* a cyclic group. What are the possible orders of g? Why?

13.a. Let H and K be subgroups of G. Prove that $H \cap K$ is a subgroup of G.

b. Demonstrate that the union of two subgroups need not be a subgroup with an example.

14. Let X be the collection of all subgroups of S_3. Prove that $\subseteq$ is a partial order on X, and draw the Hasse diagram.

15. Let $\propto$ be an antisymmetric relation on a set X. Prove that if s and t are elements of X such that $x \propto s$ and $x \propto t$ for every $x \in X$, then $s = t$.

16. Let $X = \mathbb{R}^2$ and define a binary operation $\star$ on X by setting $(x, y) \star (w, z) = (xw, xz + y)$ for any elements (x, y) and (w, z) in X. Prove that $\star$ is associative, and that X has an identity with respect to $\star$.

17. Let $\mathbb{R}^{\pm} = \{x \in \mathbb{R} \mid x \neq 0\}$, $\mathbb{R}^{+} = \{x \in \mathbb{R} \mid x > 0\}$, and $M = \{1, -1\}$, all considered as groups under multiplication. Give an explicit isomorphism $\varphi : \mathbb{R}^{+} \times M \to \mathbb{R}^{\pm}$.

18. Let G be a group of order p^2, where p is a positive prime, and let $g \in G$. Justify your answer to each part below.

a. What are the possible orders of g?

b. Suppose G is *not* a cyclic group. What are the possible orders of g?

c. If G is not a cyclic group, exactly how many elements of order p does G have?

19. Let $(X, \preceq)$ be a poset.

a. Give a precise definition of a *least element* of X.

b. Prove that a poset can have at most one least element.

20. Let $X = \{1, 2, \ldots, n\}$ and $Y = \{1, 2, 3, 4\}$. How many maps are there from X to Y? Explain.

21. Let $\sigma = (24)(35) \in S_5$ and $\theta = (12)(45) \in S_5$. Show that σ is conjugate to τ, and explain why $\mathrm{Cl}(\sigma) = \mathrm{Cl}(\tau)$.

22. Let G be a group of order p^2, where p is a positive prime.

a. Let $g \in G$ be an element of order p. Prove that $C_g(G)$ has at least p elements.

b. Prove that $|\mathrm{Cl}(g)|$ is either 1 or p.

23. Let $\gamma : S_5 \to S_5$ be the mapping $\gamma(\sigma) = (135)\sigma(153)$. Prove that γ is an isomorphism.

24. How many quinary operations are there on $X = \{1, 2, 3, 4, 5\}$?

25. Let G be a group. For $x, y \in G$, define $x \sim y$ if $x = gyg^{-1}$ for some $g \in G$. Is $\sim$ symmetric? Transitive? Justify your answers.

26.a. List the elements of each conjugacy class of the quaternion group $Q = \{1, -1, i, -i, j, -j, k, -k\}$.

b. For each element $q \in Q$, how many elements of Q commute with q?

27. Let R be the ring of 2×2 matrices with coefficients in $\mathbb{R}$. Prove that the set

$$I = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$$

is a left ideal of R, but not a right ideal.

28. Let $\varphi : R \to S$ be a ring homomorphism.

a. Prove that the image of φ is a subring of S.

b. Suppose R is unital. Prove that $\varphi(1)$ is the multiplicative identity of the image of φ.

29.a. Give an example to show that a subring of a unital ring need not be unital.

b. Give an example of a unital subring of a ring R whose multiplicative identity is not the multiplicative identity of R.

30.a. Given ideals I and J of a ring R, prove that the set $I + J = \{i + j \mid i \in I, j \in J\}$ is an ideal.

b. Suppose K is an ideal of R such that $I \subseteq K$ and $J \subseteq K$. Prove that $I + J \subseteq K$.

31.a. Let $R = \{0, 1, a, b\}$ be a commutative ring such that $R^\times = \{1, a, b\}$. Explain why R must be an integral domain. What is the characteristic of R?

b. Make addition and multiplication tables for R.

32. Let R be an integral domain of characterstic $p > 0$, and let $R' = \{k \cdot 1 \mid k \in \mathbb{Z}\}$ be the cyclic subgroup of R generated by 1. Prove that R' is a subring of R.

33. Let F be a field and $I \subseteq F$ an ideal. Prove that if $I \neq \{0\}$, then $I = F$.

34. Let $U = \{\bar{2}x \mid x \in \mathbb{Z}_{12}\}$ and $V = \{\bar{8}x \mid x \in \mathbb{Z}_{12}\}$.

a. Make addition and multiplication tables for U. Is U a subring of $\mathbb{Z}_8$? Is U an ideal of $\mathbb{Z}_8$? Justify your answers.

b. Make addition and multiplication tables for V. Is V a subring of $\mathbb{Z}_8$? If so, is it unital? If so, what is the multiplicative identity of V?

35. Let $\varphi : \mathbb{Z}_{20} \to \mathbb{Z}_{10}$ be the map defined by $\varphi(a) = \bar{5}a$.

a. Prove that φ is a ring homomorphism.

b. Prove that the kernel of φ is $(\bar{2})$, the principal ideal generated by $\bar{2} \in \mathbb{Z}_{20}$.

36. Consider the following subset of the ring $\mathbb{Z}[x]$:

$$I \;=\; \{f \in \mathbb{Z}[x] \mid f = (x^2 - 2)g \text{ for some } g \in \mathbb{Z}[x]\}$$

That is, I is the set of all multiples of the polynomial $x^2 - 2$.

a. Prove that I is a subgroup of the additive group $\mathbb{Z}[x]$.

b. Prove that I is a subring of $\mathbb{Z}[x]$.

c. Prove that I is an ideal of $\mathbb{Z}[x]$.

37. Let $R = M(3, 3, S)$ be the ring of 3×3 matrices with entries in a commutative ring S.

a. Give an example to illustrate that R is not commutative.

b. Give an example to illustrate that R has zero-divisors.

c. Prove that if S is unital, so is R.

38. Let R be an integral domain, and let F be its field of fractions. Prove that the map $\varphi : R \to F$ defined by $\varphi(r) = \frac{r}{1}$ is an injective ring homomorphism.

39. Let $a \in \mathbb{Q}$. Prove that the real number $a + \sqrt{2}$ is algebraic over $\mathbb{Q}$.

40. Let $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_m[x]$ be the map defined by $\varphi(a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0) = \bar{a}_d x^d + \bar{a}_{d-1}x^{d-1} + \cdots + \bar{a}_1 x + \bar{a}_0$ (the bar denotes reduction modulo m).

a. Prove that φ is a ring homomorphism.

b. Prove that the kernel of φ is ideal $\langle m \rangle$ consisting of all polynomials such that each coefficient is divisible by m.

41. Let R be an integral domain. Prove that $a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \in R[x]$ has a monic associate if and only if $a_d \in R^\times$.

42. Let $\varphi : \mathbb{Q}[x] \to \mathbb{R}$ be the ring homomorphism defined by $\varphi(f) = f(\sqrt{5})$. Prove that the kernel of φ is the principal ideal generated by $\langle x^2 - 5\rangle$. [**Hint:** You can use the division algorithm to show that $\ker\varphi \subseteq \langle x^2 - 5\rangle$.]

43. Find the rational roots of the following polynomials:

a. $2x^4 + 5x^3 - 5x^2 + 7x - 3$

b. $x^4 + 3x^2 + 2$

c. $8x^3 + 4x^2 - 4x - 1$

d. $\frac{1}{2}x^3 - 3x + 2$

44. Determine whether the given polynomial is irreducible in $\mathbb{Q}[x]$. Justify your answer.

a. $x^2 + 5x + 2$

b. $x^3 - 3x + 4$

c. $x^3 + x^2 - 2x - 1$

44.a. Let $f = x^5 + 2x^4 + x^3 + 2x^2 + x + 2 \in \mathbb{Q}x$ and $g = x^4 - x \in \mathbb{Q}[x]$. Find a monic polynomial $h \in \mathbb{Q}[x]$ such that $\langle f, g\rangle = \langle h\rangle$.

b. Express h in the form $af + bg$ for some polynomials $a, b \in \mathbb{Q}[x]$.

45. Let F be a field, and let $f, g \in F[x]$ be polynomials such that $\langle f, g\rangle = F[x]$. Prove that $\langle f\rangle \cap \langle g\rangle = \langle fg\rangle$.

46. Use the Fundamental Theorem of Algebra and mathematical induction to prove that every monic polynomial $f \in \mathbb{C}[x]$ of degree d factors into a product $f = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_d)$ for some complex numbers $\alpha_1, \alpha_2, \ldots, \alpha_d \in \mathbb{C}$.

47. Determine if the given polynomial is irreducible in $\mathbb{R}[x]$.

a. $3x^2 - 2x + 5$

b. $x^2 + x + 1$

c. $2x^2 + 8x + 1$

d. $x^2 + x - 1$

c. $2x^2 + 8x - 1$

48. Let $F \subseteq K$ be fields and let $\alpha, \beta \in K$ be algebraic over F. Suppose α and β have the same minimal polynomial $f \in F[x]$. Prove that $F[\alpha]$ is isomorphic to $F[\beta]$.

49. Find the minimal polynomial of $\sqrt{2} + i$

a. over $\mathbb{C}$.

b. over $\mathbb{R}$.

c. over $\mathbb{Q}$.