Math 558 Spring 2009

Review for final

Warning: The questions below only cover material since the second exam. You are also responsible for most of the material covered in the review questions for the two in-class exam. About $\frac{1}{3}$ of the exam will be on old material.

I will not ask you about formulas for zeroes of cubics or ruler and compass constructions.

Problems marked * are from new material that wasn't on the homework.

I. Calculations

1. Find all subgroups of S_3. Which of them are normal?
2. (a) Find all subgroups of $G = (\mathbb{Z}_{12}, +)$.
   (b) For each subgroup H in (a), what are the cosets in G/H?
   (c) For each subgroup H in (a), what standard group is G/H isomorphic to?
3. Let $G = (\mathbb{Z}_{17}^{+}, \cdot)$.
   (a) How many subgroups of G are there?
   (b) What are the orders of the subgroups of G?
   (c) $(\mathbb{Z}_n, +)$ is a homomorphic image of G for exactly which n?
   (d) If $G/H \cong (\mathbb{Z}_n, +)$, how big is H?
4. (a) Find the smallest n so $(\mathbb{Z}_{17}^{+}, \cdot) =< n >$.
   (b) Find an isomorphism between $(\mathbb{Z}_{17}, \cdot)$ and $(\mathbb{Z}_{16}, +)$.
   (c) Find a homomorphism from $(\mathbb{Z}_{17}, \cdot)$ to $(\mathbb{Z}_4, +)$.
   (d) What is the kernel of the homomorphism in (c)?
5. (a) Find an isomorphism between $(GF(2, x^2 + x + 1), +)$ and K.
   (b) Find a homomorphism from $(GF(2, x^2 + x + 1), +)$ to $(\mathbb{Z}_2, +)$.
   (d) What is the kernel of the homomorphism in (b)?

* 6. Let f be a homomorphism from $(\mathbb{Z}_{15}, +)$ to a mystery group J where $\ker(f) = \{0, 5, 10\}$. What is J?[1]

* 7. Same as #6, except f goes from $(\mathbb{C}, +)$ and $\ker(f) = \mathbb{R}$.

II. Short answer: don't give reasons unless asked.

1. Let $\sigma, \tau \in S_n$ for some n.
   (a) Give conditions on σ, τ so $o(\sigma\tau) = o(\sigma)(\tau)$.
   (b) Give an example where $o(\sigma\tau) \neq o(\sigma)(o(\tau)$.
2. Does S_7 have a subgroup of size 13? A homomorphic image of size 13? Explain in one phrase.
4. True or false? No proofs needed if true, but if false give a counterexample.
   (a) Every cyclic group is commutative.
   (b) Every commutative group is cyclic.

[1] up to isomorphism of course

(c) Every element in a finite group is a root of unity.

(d) If $n < m$ then S_n is a subgroup of S_m.

(e) If $n < m$ then S_n is a normal subgroup of S_m.

(f) If G is commutative, then every subgroup of G is normal.

(g) If H is a subgroup of G and H is commutative, then H is normal.

(h) Every normal subgroup is commutative.

* 5. Define $\mathbb{R}^> = \{x \in \mathbb{R} : x > 0\}$. Let $f : \mathbb{R}^+ \to \mathbb{R}^>$ be a homomorphism from $(\mathbb{R}, \cdot)$ to $(\mathbb{R}^>, \cdot)$ so $\ker(f) = \{1, -1\}$. Which of the following could be f? No reasons need be given. [Note: there might be more than one correct answer, or there might be none.]

(i) $f(x) = x^2$

(ii) $f(x) = x^3$

(iii) $f(x) = x^4$

(iv) $f(x) = x^2 + 1$

(v) $f(x) = e^x$

6. Q and D_4 are both non-commutative, and both have order 8. Are they isomorphic or not? Give reasons.

7. In the proof that if k, n are relatively prime then the map $f(x) = kx$ is an automorphism of $(\mathbb{Z}_n, +)$, most people didn't explicitly say where the hypothesis of relatively prime was used. Where is it used?

8. When is $\sqrt[n]{1}$ a subgroup of $\sqrt[m]{1}$?

9. Each of the following is not a group. Why or why not?

(a) $(F[x]^+, \cdot)$ where F is a field.

(b) $(\mathbb{Z}^+, \cdot)$.

10. For each of the following $G, S \subset G$, say what $< S >$ is:

(a) $G = (\mathbb{Z}_{12}, +), S = \{2\}$.

(b) $G = (\mathbb{Z}_{12}, +), S = \{6, 9\}$.

(c) $G = (\mathbb{R}^+, \cdot), S = \mathbb{Z}^+$.

(d) $G = (\{\text{roots of unity in } \mathbb{C}\}, \cdot), S = \{1, i, \omega)\}$.[2]

III. Proofs

1. Prove that if $n > 2$ then the subgroup $\{Id, (12)\}$ is not a normal subgroup of S_n.

2. Let p be a prime, P irreducible over $\mathbb{Z}_p$, $\deg P > 1$.

(a) What is the maximum order of an element of $(GF(p, P), +)$?

(b) Prove that $(GF(p, P), +)$ is not cyclic

3. Show that a homomorphism f is an isomorphism iff its kernel is $\{e\}$.

4. In class we said the kernel of a homomorphism was $\{z \in \mathbb{C} : |z| = 1\}$. Prove that this actually is a subgroup of $(\mathbb{C}, \cdot)$.

5. Let G be a group and $g \in G$. The *conjugacy class* $C(g) = \{h \in G : \exists k \in G\ h = kgk^{-1}\}$.

[2] Recall that ω is one of the cube roots of unity.

(a) Prove that $C(g) = C(h)$ iff $h \in C(g)$

(b) Prove that for all $g, h \in G$, gh is conjugate to hg.

6. Let G be a group. Let $H = \{g \in G : \forall h \in G \; gh = hg\}$.

(a) Prove that H is a group. [H is called the commutator subgroup of G.]

(b) What's the commutator subgroup of Q?

(c) What's the commutator subgroup of S_3?

7. Let R be a ring and let $I(R) = \{a \in R : a$ has a multiplicative inverse a^{-1} in $R\}$.

(a) If $R = \mathbb{Z}$, what's $I(R)$?

(b) [do this only if you've had linear algebra] If R is the set of $n \times n$ matrices with coefficients in a field F, what is $I(R)$?

(c) Prove that $(I(R), \cdot)$ is a group, where $\cdot$ is multiplication in R.

IV. Proofs to know in advance

1. Prove that if a group G has order p, where p is prime, then the only subgroups of G are G and $\{Id\}$.
2. Prove that if a group G is commutative, then every subgroup of G is normal.
3. Prove that if H is a normal subgroup of a group G and $g \in G$ then $o(gH)$ divides $o(g)$.
4. Prove that every quotient group of a cyclic group is cyclic.
5. Prove that the order of a subgroup of G divides the order of G. [Use the short proof.]
6. Prove that every group is isomorphic to a group of permutations.