Reading Questions
Math 433, Abstract Algebra I
Fall 2011

Chapter 1, Preliminaries

1. What do relations and mappings have in common?
2. What makes relations and mappings different?
3. State carefully the three defining properties of an equivalence relation. In other words, do not just *name* the properties, give their definitions.
4. What is the big deal about equivalence relations? (Hint: Partitions.)
5. Describe a general technique for proving that two sets are equal.

Chapter 2, The Integers

1. Use Sage to express 123456792 as a product of prime numbers.
2. Find the greatest common divisor of 84 and 52.
3. Find integers r and s so that $r(84) + s(52) = \gcd(84, 52)$.
4. Explain the use of the term "induction hypothesis."
5. What is Goldbach's Conjecture? And why is it called a "conjecture"?

Chapter 3, Groups

1. In the group $\mathbb{Z}_8$ compute (a) $6 + 7$, (b) 2^{-1}
2. In the group $U(16)$ compute (a) $5 \cdot 7$, (b) 3^{-1}
3. State the definition of a group.
4. Explain a single method that will decide if a subset of a group is itself a subgroup.
5. Explain the origin of the term "abelian" for a commutative group.

Chapter 4, Cyclic Groups

1. What is the order of the element 3 in U(20)?
2. What is the order of the element 5 in U(23)?
3. Find three generators of $\mathbb{Z}_8$.
4. Find three generators of the 5^{th} roots of unity.
5. Show how to compute $15^{40} \pmod{23}$ efficiently by hand. Check your answer with SAGE.

Chapter 5, Permutation Groups

1. Express $(1\,3\,4)(3\,5\,4)$ as a cycle, or a product of disjoint cycles.
2. What is a transposition?
3. What does it mean for a permutation to be even or odd?
4. Describe another group that is fundamentally the same as A_3.
5. Write the elements of the symmetry group of a pentagon using permutations in cycle notation.

Chapter 6, Cosets and Lagrange's Theorem

1. State Lagrange's Theorem in your own words.
2. Determine the left cosets of $\langle 3 \rangle$ in $\mathbb{Z}_9$.
3. The set $\{(), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ is a subgroup of S_4. What is its index in S_4?
4. Suppose G is a group of order 29. Describe G.
5. $p = 137909$ is a prime. Explain how to compute $57^{137909} \pmod{137909}$ without a calculator.

Chapter 9, Isomorphisms

1. Determine the order of $(1, 2)$ in $\mathbb{Z}_4 \times \mathbb{Z}_8$.
2. List three properties of a group that are preserved by an isomorphism.
3. Find a group isomorphic to $\mathbb{Z}_{15}$ that is an external direct product of two non-trivial subgroups.
4. Explain why we can now say "*the* infinite cyclic group"?
5. Compare and contrast external direct products and internal direct products.

Chapter 10, Normal Subgroups and Factor Groups

1. Let G be the group of symmetries of an equilateral triangle, expressed as permutations of the vertices numbered $1, 2, 3$. Let H be the subgroup $H = \langle\{(1\ 2)\}\rangle$. Build the left and right cosets of H in G.
2. Based on your answer to the previous question, is H normal in G? Explain why or why not.
3. $8\mathbb{Z}$ is a normal subgroup in $\mathbb{Z}$. In the factor group $\mathbb{Z}/8\mathbb{Z}$ perform the computation $(3 + 8\mathbb{Z}) + (7 + 8\mathbb{Z})$.
4. List two statements about a group G and a subgroup H that are equivalent to "H is normal in G."
5. In your own words, what is a factor group?

Chapter 7, Introduction to Cryptography

1. Use the `euler_phi()` function in Sage to compute $\phi(893, 456, 123)$.
2. Use the `power_mod()` function in Sage to compute $7^{324} \pmod{895}$.
3. Explain the mathematical basis for saying: the encoding fuction of RSA is simple computationally, while the decoding function is hard computationally.
4. Explain how in RSA message encoding differs from message verification.
5. Explain how one could be justified in saying that Diffie and Hellman's proposal in 1976 was "revolutionary."

Chapter 11, Homomorphisms

1. Consider the function $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ defined by $\phi(x) = x + x$. Prove that ϕ is a group homomorphism.
2. For ϕ defined in the previous question, explain why ϕ is not a group isomorphism..
3. Compare and contrast isomorphisms and homomorphisms.
4. State the definition of a simple group. What is interesting about simple groups historically?
5. "For every normal subgroup there is a homomorphism, and for every homomorphism there is a normal subgroup." Explain the (precise) basis for this (vague) statement.

Chapter 13, The Structure of Groups

1. How many abelian groups are there of order $200 = 2^3 5^2$?
2. How many abelian groups are there of order $729 = 3^6$?
3. Find a subgroup of order 6 in $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.
4. It can be shown that an abelian group of order 72 contains a subgroup of order 8. What are the possibilities for this subgroup?
5. What is a principal series of the group G?

Chapter 14, Group Actions

1. Give an informal description of a group action.
2. Describe the class equation.
3. What are the groups of order 49?
4. How many switching fuctions are there with 5 inputs?
5. The "Historical Note" mentions the proof of Burnside's Conjecture. How long was the proof?

Chapter 15, The Sylow Theorems

1. State Sylow's First Theorem.
2. How many groups are there of order 69? Why?
3. Give two descriptions, different in character, of the normalizer of a subgroup.
4. What's all the fuss about Sylow's Theorems?
5. Name one of Sylow's academic great-great-great-great-great-great-grandchildren.
   (That's $(\text{great-})^6$grand-children.)