Math 405 – Abstract Algebra
Spring 2018
Final Exam Part 1
Due: Tuesday, May 1, 11:30am

In doing these problems, you may refer freely to your Math 405 class notes, the course textbook, and to any of your previous homework or exam for this course, including comments on them from the instructor. You are not to use any other references or tools, including web-based ones. You are not to discuss your work with anyone other than your instructor. In particular you should not discuss the problems with any students, whether they are enrolled in this class or not, or any professors other than the instructor.

If anything about these instructions is unclear to you, it is your responsibility to see me for clarification.

Any form of cheating on this exam will be dealt with seriously. At a minimum, the full take-home examination will receive a score of zero. Depending on my concern with the extent of cheating, any incident may result in a course grade of F, and I may also request a University Disciplinary and Honor Code Committee hearing which could result in suspension or expulsion. Please note that evidence of collaboration on work in mathematics is usually obvious, so even if your personal honor is worth nothing to you, cheating is a foolish risk to take.

When writing your solutions, present your arguments with good mathematical style. Clearly state as theorems or propositions anything you prove. Organization and clarity of presentation will be factors in grades. If you refer to a result in the text in an argument, you should specify both theorem number/name and page number.

If you get stuck on a problem, give yourself time to try different approaches. If you think it might be helpful, you can discuss the problem with me. I will not give you solutions or read your solutions for correctness before they are turned in, but may be able to help you see your difficulties in order to overcome them. Though I will answer brief clarification questions by e-mail, for anything more complicated you must see me in person.

The problems are not in order of difficulty, and you may not be able to do all parts of all problems. On multipart problems, you may use previous parts to complete later parts, whether or not you were able to find solutions to the previous ones.

Solutions may be turned in either at 704F Gruening or the mailboxes in the DMS office in Chapman.

Sign and date the statement on the last page of this handout, and attach it to the front of your solutions when you turn them in.

1. The motivation for this problem is to understand how the ring of the integers, $\mathbb{Z}$, can be rigorously defined/invented from the set of natural numbers, $\mathbb{N} = \{1, 2, \dots\}$, and the operations of addition and multiplication on $\mathbb{N}$ only.

   To obtain a more general result, suppose a set S is endowed with binary operations of addition and multiplication, where addition is associative, commutative, and the distributive laws hold. Further assume that the cancellation law for addition holds, i.e.,

   $$\text{If } a + c = b + c, \text{ then } a = b.$$

   Then we will construct a ring R which contains (a subset isomorphic to) S. In many ways, this parallels the construction of the field of fractions from an integral domain, which might review if you need inspiration.

   The key idea in constructing R is to use an ordered pair (a, b) to "represent" what we would like to think of as $a - b$ (which has no meaning yet, since $-b$ may not exist). But since we need $a - b = c - d$ whenever $a + d = b + c$, we must make (a, b) "equal to" (c, d) through an equivalence relation.

   (a) Let $T = S \times S$, and define a relation on T by $(a, b) \sim (c, d)$ when $a + d = b + c$, Show this is an equivalence relation.

   (b) Let $R = T/\sim$ denote the set of equivalence classes of T under $\sim$. For equivalence classes $\alpha, \beta \in R$, define $\alpha+\beta$ to be the class of $(a+c, b+d)$ where (a, b) is any element of α and (c, d) is any element of β. Show this operation of addition on R is a well-defined commutative binary operation on R.

   (c) Show R with addition is a group.

   (d) Using that (a, b) "represents" $a - b$, define an appropriate operation of multiplication on R, and show it is well-defined. (Do not assume that multiplication on S is commutative.)

   (e) Show R with addition and multiplication is a ring. (You may show only the left or right distributive law holds, and say the other can be shown 'similarly'.)

   (f) Define the function $\phi : S \to R$ by $\phi(s)$ is the class of $(s+s, s)$. Show ϕ is one-to-one, and operation preserving for both addition and multiplication.

2. Boolean rings are named after the George Boole (1815–1864), an English mathematician who did early work in set theory and logic.

   Let X be any non-empty set. Then the *Boolean ring* $\mathcal{B}(X)$ *associated to* X is the set of all subsets of X, together with operations of addition and multiplication defined by

   $$\begin{aligned} A + B &= (A \smallsetminus B) \cup (B \smallsetminus A) = \{x | x \in A \text{ or } B \text{ but not both}\} \\ AB &= A \cap B, \end{aligned}$$

   for all $A, B \in \mathcal{B}(X)$. (The addition operation is, in other contexts, also called the *symmetric difference* of A and B. It is related to 'exclusive or' in the same way that the union of sets is related to 'or' and the intersection of sets is related to 'and'.)

   (a) To understand a concrete example, for $X = \{1, 2, 3\}$ list the elements of $\mathcal{B}(X)$ and give Cayley tables for the two operations.

   (b) Prove that, for any set X, $\mathcal{B}(X)$ is a commutative ring.

   (c) Prove that, for any set X, $\mathcal{B}(X)$ has characteristic 2.

   (d) Prove that, for any set X, $\mathcal{B}(X)$ has a 1, and contains no units other than 1.

(e) For $X = \{1, 2, 3, \ldots, n\}$, define

$$\phi : \mathcal{B}(X) \to \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{n}$$

so that $\phi(A)$ is the vector whose ith entry is 1 if $i \in A$, and 0 if $i \notin A$ (e.g., for $n = 4$, $\phi(\{1, 3\}) = (1, 0, 1, 0)$). Show ϕ is an isomorphism.

3. The *quaternions* $\mathbb{H}$ were found/invented on October 16, 1843, by William Hamilton, who then carved the basic rules of their algebra into the bridge in Dublin on which he was walking at the time. As a set,

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\},$$

where i, j, k are simply three different symbols. Addition is defined by

$$(a_1 + b_1 i + c_1 j + d_1 k) + (a_2 + b_2 i + c_2 j + d_2 k) = (a_1 + a_2) + (b_1 + b_2)i + (c_1 + c_2)j + (d_1 + d_2)k.$$

Multiplication is defined so that a) all real numbers commute with i, j, k; b) both left and right distributive laws hold; and c)

$$\begin{gathered} i^2 = j^2 = k^2 = -1, \\ ij = k,\ jk = i,\ ki = j, \\ ji = -k,\ kj = -i,\ ik = -j. \end{gathered}$$

This makes $\mathbb{H}$ a non-commutative ring with a 1, though we won't prove that. Note that i, j, k all behave like square roots of -1, so you might think of $\mathbb{H}$ as some sort of 'hyper-complex' numbers.

(a) Show that if

$$(a_1 + b_1 i + c_1 j + d_1 k)(a_2 + b_2 i + c_2 j + d_2 k) = a_3 + b_3 i + c_3 j + d_3 k$$

then $a_3 = a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2$, and give similar formulas for b_3, c_3 and d_3.

(b) Show that the polynomial equation $x^2 + 1 = 0$ has infinitely many solutions in $\mathbb{H}$, by finding infinitely many solutions of this equation of the form $bi + cj$.

(c) For rings R and S, an *anti-homomorphism* is a map $\psi : R \to S$ such that

$$\begin{aligned} \psi(r_1 + r_2) &= \psi(r_1) + \psi(r_2) \\ \psi(r_1 r_2) &= \psi(r_2)\psi(r_1). \end{aligned}$$

Show that $\phi : \mathbb{H} \to \mathbb{H}$ defined by $\phi(a + bi + cj + dk) = a - bi - cj - dk$ is an anti-automorphism of $\mathbb{H}$, but is not an automorphism.

For $\alpha \in \mathbb{H}$, $\phi(\alpha)$ is sometimes referred to as *quaternionic conjugate* of α, and is usually denoted by $\bar{\alpha}$

(d) The *quaternionic norm* of $\alpha \in \mathbb{H}$ is defined by $N(\alpha) = \alpha\bar{\alpha}$.

i. Show $N(\alpha) \in [0, \infty) \subset \mathbb{R}$; and $N(\alpha) = 0$ if, and only if, $\alpha = 0$.

ii. It can be (painfully) verified using part (a) that $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in \mathbb{H}$. Do not verify it, but use this fact to show that $\mathbb{H}$ has no zero-divisors.

iii. Show all $\alpha \neq 0$ have inverses given by $\alpha^{-1} = N(\alpha)^{-1}\bar{\alpha}$. (Why does the right side of this formula not assume an inverse exists in $\mathbb{H}$?)

Thus, except for its non-commutativity, $\mathbb{H}$ has all the necessary properties to be a field. A ring of this sort is usually called a *division ring* or a *skew field*.

(e) $\mathbb{H}$ is isomorphic to a subring of the 2×2 complex matrices $M_2(\mathbb{C})$. To see this, since the identity matrix I is the 1 of $M_2(\mathbb{C})$, we must choose matrices whose squares are $-I$ to play the roles of i, j, k.

i. Show $B = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ and $C = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ satisfy $B^2 = C^2 = -I$.

ii. Choose an appropriate matrix D, and define $\psi : \mathbb{H} \to M_2(\mathbb{C})$ by

$$\psi(a + bi + cj + dk) = aI + bB + cC + dD.$$

Prove ψ is an injective homomorphism, but is not surjective.

iii. Show the norm for $\mathbb{H}$ is related to common matrix calculations by showing $N = \det \circ \psi$. (This can be used to more easily show $N(\alpha\beta) = N(\alpha)N(\beta)$, but you don't need to do so.)

iv. The quaternionic conjugate is also related to familiar notions. Find an anti-automorphism $F : M_2(\mathbb{C}) \to M_2(\mathbb{C})$ such that $F \circ \psi = \psi \circ \phi$.

4. (a) Show that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain using the norm $N(a + b\sqrt{-2}) = a^2 + 2b^2$, by imitating the proof of the analogous fact for $\mathbb{Z}[\sqrt{-1}]$ that is in the textbook and was presented in class.

(b) Explain where a similar attempt at a proof that $Z[\sqrt{-3}]$ is a Euclidean domain fails.

(c) Prove that $Z[\sqrt{-3}]$ is not a Euclidean domain. (Hint: what do you know about factorization in $Z[\sqrt{-3}]$?)

In working on this examination, I have followed all the rules laid out on the examination handout and in the course syllabus. In particular, I have discussed this work with no one other than the course instructor, and used no reference materials other than the course textbook, my own course notes, and my own graded homework assignments.

All the work presented here is fully my own.

Signed: _____ Date:_____