Clark University

Math 225 Modern Algebra

First Test

October 2017

You may refer to one sheet of notes on this test. Points for each problem are in square brackets. Write your answers in the bluebook provided. You may do the problems in any order that you like, but please start your answers to each problem on a separate page of the bluebook. Please write or print clearly.

1. [20] On fields. Recall the definition of a field. A *field* F consists of

1. a set, also denoted F and called the *underlying set* of the field;
2. a binary operation $+ : F \times F \to F$ called *addition*, which maps an ordered pair $(x, y) \in F \times F$ to its *sum* denoted $x + y$;
3. another binary operation $\cdot : F \times F \to F$ called *multiplication*, which maps an ordered pair $(x, y) \in F \times F$ to its *product* denoted $x \cdot y$, or more simply just xy; such that
4. addition is commutative, that is, for all elements x and y, $x + y = y + x$;
5. multiplication is commutative, that is, for all elements x and y, $xy = yx$;
6. addition is associative, that is, for all elements x, y, and z, $(x + y) + z = x + (y + z)$;
7. multiplication is associative, that is, for all elements x, y, and z, $(xy)z = x(yz)$;
8. there is an additive identity, an element of F denoted 0, such that for all elements x, $0 + x = x$;
9. there is a multiplicative identity, an element of F denoted 1, such that for all elements x, $1x = x$;
10. there are additive inverses, that is, for each element x, there exists an element y such that $x + y = 0$; such a y is called the *negation* of x;
11. there are multiplicative inverses of nonzero elements, that is, for each nonzero element x, there exists an element y such that $xy = 1$; such a y is called a *reciprocal* of x;
12. multiplication distributes over addition, that is, for all elements x, y, and z, $x(y + z) = xy + xz$; and
13. $0 \neq 1$.

Carefully prove that 0 times any element in a field is 0, $0x = 0$, using only the definition above and no other properties of a field (unless you prove them as well). Justify every statement and equation. Write full sentences.

2. [15; 5 points each part] On rings.

a. Give an example of a ring R and two elements x and y in R, neither of which is 0, but the product xy of the two elements is 0.

b. Give an example of a ring of characteristic 0.

c. Give an example of a subring of the field $\mathbf{R}$ of real numbers other than $\mathbf{R}$ itself.

3. [20; 5 points each part] On groups. For each of the following, state if it is a group or not. If not, explain why not, but if so, you don't have to give a reason why.

a. The set $\{1, -1, i, -i\}$ of four complex numbers under addition.

b. The set $\{1, -1, i, -i\}$ of four complex numbers under multiplication.

c. The set of six functions including $f(x) = \dfrac{1}{x}$, $g(x) = 1 - x$, $h(x) = \dfrac{1}{1-x}$, $i(x) = x$, $k(x) = \dfrac{x-1}{x}$, and $\ell(x) = \dfrac{x}{x-1}$ under composition.

d. The set of 2×2 matrices in $M_2(\mathbf{R})$ with positive determinants under matrix multiplication.

4. [16; 8 points each part] On number theory.

a. Draw a Hasse diagram of the divisors of 30.

b. Use the Euclidean algorithm to show that the greatest common divisor of 105 and 154 is 7. Show your work.

5. [15] On ordered fields. Recall that an order on a field F is determined by a subset P whose elements are called positive such that (1) F is partitioned into three parts: P , $\{0\}$, and $N = \{x \in F \,|\, x \in P\}$, (2) the sum of two positive elements is positive; and (3) the product of two positive elements is positive.

Explain in your own words why a field of prime characteristic p cannot have an order of this kind.

6. [16; 8 points each part] On finite fields. We have had examples and exercises on finite fields. The Galois field $GF(2)$ is the ring $\mathbf{Z}_2$ of integers modulo 2. In this exercise you'll construct the Galois field $GF(8)$ as an extension of $\mathbf{Z}_2$.

a. Find at least one of the following cubic polynomials that has no root in $\mathbf{Z}_2$: x^3, $x^3 + 1$, $x^3 + x$, $x^3 + x + 1$, $x^3 + x^2$, $x^3 + x^2 + 1$, $x^3 + x^2 + x$, $x^3 + x^2 + x + 1$. That is to say, if $f(x)$ is the polynomial, its value at neither of the two elements of $\mathbf{Z}_2$ is equal to 0.

Now let $f(x)$ be that polynomial you found in part a. Let F be the 3-dimensional vector space over $\mathbf{Z}_2$ of 8 elements where each element is written as $ax^2 + bx + c$ with a, b, and c each in $\mathbf{Z}_2$. Define multiplication on F so that $f(x) = 0$. (So, for instance, if $f(x) = x^3 + x^2 + x + 1$, then $x^3 = -x^2 - x - 1$.)

b. With your choice of $f(x)$, F will be a field where every nonzero element has a reciprocal. Determine the reciprocal of x in F, that is, find some polynomial whose product with x is equal to 1 modulo $f(x)$.