Math 125 Modern Algebra

First Test Anaswers

March 2017

Scale. 80–100 A, 60–79 B, 40–59 C. Median 72.

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.

There are many possible proofs. Here is one.

Let x be an element of the field. Since 0 is the additive identity (8), therefore $0 + 0 = 0$. Multiply that equation by x. Then $x(0+0) = x0$. Since multiplication distributes over addition (12), therefore $x0 + x0 = x0$. Let y be the additive inverse of $x0$ (10) so that $x0 + y = 0$. Add y to each side of the equation $x0+x0 = x0$. Then $(x0+x0)+y = x0+y$. Since addition is associative (6), therefore $x0 + (x0 + y) = x0 + y$. But $x0 + y = 0$, so $x0 + 0 = 0$. And since 0 is the additive identity (8 again), therefore $x0 = 0$. Finally, multiplication is commutative (5), so $0x = 0$. Q.E.D.

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.

There are many. One that was mentioned in class is the ring $\mathbf{Z}_6$ where $x = 2$ and $y = 3$.

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

Some examples: $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$.

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

$\mathbf{Z}$ and $\mathbf{Q}$ are both subrings of $\mathbf{R}$.

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.

It is not a group under addition. It doesn't have 0. Also, it's not closed under addition.

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

It is a group. It's a cyclic group of four elements.

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.

It is a group. This is one of the examples discussed in class.

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

It is a group. The identity matrix is in this set, and it's closed under multiplication and inverses. It's a subgroup of the general linear group $GL(2, R)$

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

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

There are eight divisors of 30. The Hasse diagram has 1 at the bottom; 2, 3, and 5 above 1; 6 above 2 and 3; 10 above 2 and 5; 15 above 3 and 5; and 30 at the top.

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

Since $154 - 105 = 49$, therefore $\text{GCD}(105, 154)$ is equal to $\text{GCD}(105, 49)$. Subtracting 49 twice from 105 gives 7, so $\text{GCD}(105, 49)$ is equal to $\text{GCD}(7, 49)$. Since 7 divides 49, therefore 7 is the greatest common divisor.

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.

Suppose there were an order of this kind for a field prime characteristic p. Since 1 is positive, and positive elements are closed under addition, therefore $1+1+\cdots+1$ is positive. But when there are p terms in the sum, that sum is equal to 0 which is not positive. That contradicts condition (1). Therefore there is no such order.

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.

0 will be a root of any of those polynomials that don't have the constant 1. That leaves the four polynomials that do have the constant 1. 1 will be a root of any polynomial with 2 or 4 terms. That leaves two polynomials: x^3+x+1 and x^3+x^2+1. Either one will do.

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 $f(x)$.

Let $f(x) = x^3+x+1$. Then $x^3+x+1 = 0$ which can be rewritten $x^3+x = 1$. Divide by x to conclude $\dfrac{1}{x} = x^2+1$.

(In fact the seven nonzero elements of $GF(8)$ form a cyclic group under multiplication.)

n	0	1	2	3	4	5	6
x^n	1	x	x^2	$x+1$	x^2+x	x^2+x+1	x^2+1