Math 110 Homework 9 Solutions

March 12, 2015

1. For this question, refer to your handout on Field Axioms.

   (a) State which of the examples in Section 2 are fields, and for each of the non-fields, cite at least one axiom that fails. No proof needed.

   (b) Using the definition of a multiplicative inverse, prove that for any nonzero $a \in \mathbb{F}$, $(a^{-1})^{-1} = a$.

   (c) Using the field axioms, prove that $a \cdot 0 = 0$ for any $a \in \mathbb{F}$. *Hint*: Expand $a \cdot (1 + 0)$ in two ways.

   (d) Using the field axioms and Part (b), prove that fields have no (nonzero) zero divisors.

   (e) Let $\mathbb{F}$ be a finite field with multiplicative identity 1. We define the *characteristic* of $\mathbb{F}$ to be the smallest positive number n such that the sum

   $$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}$$

   is equal to the additive identity zero. Prove that, if $\mathbb{F}$ is finite, then it has a finite characteristic n. Further prove that the characteristic of $\mathbb{F}$ must be prime.

   Note: For some infinite fields, such as $\mathbb{Q}$ and $\mathbb{R}$, the sum of any number of 1's is nonzero. These fields are said to have *characteristic zero.*

   Note: For a field $\mathbb{F}$, it is standard to refer to the sum

   $$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}$$

   by the number n. With this convention, we can identify a copy of the integers $\mathbb{Z}$ in any field of characteristic zero, and a copy of the field $\mathbb{Z}/p\mathbb{Z}$ in any field of characteristic p.

   Solution:

   (a) The integers $\mathbb{Z}$ are not a field because there are not multiplicative inverses. $\mathbb{Q}$ and $\mathbb{R}$ and fields. $\mathbb{R}_{>0}$ is not a field because there are not additive inverses. The complex numbers are a field. Three by three matrices are not because some do not have multiplicative inverses. The invertible matrices are not because there is no way to add them. $\mathbb{Z}/p\mathbb{Z}$ is a field, $\mathbb{Z}/n\mathbb{Z}$ is not a field if n is not prime because multiplicative inverses do not exist. $(\mathbb{Z}/n\mathbb{Z})^\times$ is not a field because there is no way to add elements. $\mathbb{Q}[x]$ is not a field because there are no multiplicative inverses for a polynomial like x.

   (b) A multiplicative inverse for a satisfies $aa^{-1} = 1$. Let $b = a^{-1}$. A multiplicative inverse for b satisfies $b^{-1}b = 1$, ie $(a^{-1})^{-1}a^{-1} = 1$. But taking

   $$(a^{-1})^{-1}a^{-1} = aa^{-1}$$

   and multiplying by a gives $((a^{-1})^{-1}a^{-1})a = (aa^{-1})a$. By associativity and the definition of multiplicative inverse, we see that $(a^{-1})^{-1} \cdot 1 = a \cdot 1$. Using the definition of a multiplicative identity, we see that $(a^{-1})^{-1} = a$.

(c) Consider $a \cdot (1+0)$. We know $1+0=1$ by the definition of additive identity, and by the definition of multiplicative identity we see $a \cdot 1 = a$. On the other hand, $a \cdot (1+0) = a \cdot 1 + a \cdot 0$ by distributivity. By the definition of multiplicative identity, we have $a \cdot 1 = a$. Comparing, we see

$$a = a + a \cdot 0.$$

Adding $-a$ on the right, invoking associativity, and the definition of additive inverse, we obtained

$$0 = 0 + a \cdot 0.$$

By the definition of an additive identity, we see $a \cdot 0 = 0$.

(d) Suppose $a \cdot b = 0$ and $b \neq 0$. Then b has a multiplicative inverse, so $(a \cdot b) \cdot b^{-1} = 0 \cdot b^{-1}$. Using associativity and the definition of multiplicative inverse, the left side is $a \cdot 1$ which is a by the definition of multiplicative identity. The right side is 0 by commutativity and the previous part. Thus $a = 0$, so a field has no zero divisors.

(e) For a positive integer n define $n \cdot 1$ to be the sum of n copies of 1. If a field is finite, consider the infinitely many expressions of the form $\{n \cdot 1\}_{n \in \mathbb{N}}$. There must be overlap, so for some n and m we must have $n \cdot 1 = m \cdot 1$. Say $n > m$. Hence using additive inverses to cancel ones we see $(n-m) \cdot 1 = 0$. Thus the field has finite characteristic.

Let a field have finite characteristic n. Suppose we can factor $n = m' \cdot m''$. Then consider $(m' \cdot 1)(m'' \cdot 1)$. By expanding using the distributive law and the fact that $1 \cdot 1 = 1$, we see that this product is just a sum of n ones, ie $n \cdot 1$. This is 0. But a field has no zero divisors, so without loss of generality we may assume $m' \cdot 1 = 0$. But the characteristic n is the minimal positive integer with this property, so $n = m'$. Thus we cannot factor n non-trivially. Thus n is prime.

2. Let $\mathbb{F}_p$ denote the field $\mathbb{Z}/p\mathbb{Z}$ for some positive prime p. Let $\mathbb{F}_p[x]$ denote the set of polynomials in the variable x with coefficients in $\mathbb{F}_p$.

(a) What is an *irreducible* polynomial $P(x)$? Show by example that polynomials that are irreducible over the integers may not be irreducible over $\mathbb{F}_p[x]$, and that polynomials that are irreducible over $\mathbb{F}_p[x]$ may not be irreducible over $\mathbb{F}_q[x]$ for $q \neq p$.

(b) Let $P(x) \in \mathbb{F}_p[x]$ be a polynomial of degree d. Define the *congruence classes* of $\mathbb{F}_p[x]$ modulo $P(x)$, and compute how many congruence classes there are.

(c) Explain how to construct a finite field with p^k elements (Chapter 3.11).

(d) Explain why the object you've constructed is a field. Specifically, explain why the one non-obvious field axiom holds: nonzero elements have multiplicative inverses.

(e) Remark that every polynomial in $P(x) \in \mathbb{F}_p[x]$ defines a *polynomial function* on $\mathbb{F}_p$, mapping $b \in \mathbb{F}_p$ to the congruence class $P(b) \in \mathbb{F}_p$ obtained by substituting $x = b$. Give an example of how two different polynomials can define the same function on $\mathbb{F}_p$ (*Hint*: If $a \in \mathbb{F}_p$, what is $a^p \pmod{p}$?) Note that the two polynomials in your example are still considered distinct elements in $\mathbb{F}_p[x]$, even if they define the same function $\mathbb{F}_p \to \mathbb{F}_p$.

Solution:

(a) An irreducible polynomial is a polynomial such that if $P(x) = q(x)r(x)$ then either $q(x)$ or $r(x)$ is a unit. (A unit is an element with a multiplicative inverse. In $\mathbb{F}_p[x]$, the units are non-zero constants.) In other words, it is impossible to factor $P(x)$ in a non-trivial way. Consider $x^2 + 1$. This is irreducible if and only if there is no root. So it is irreducible over $\mathbb{Z}$, but there is a root modulo 5 so it is reducible in $\mathbb{F}_5[x]$. Now consider the polynomial $x^2 + 2 \in \mathbb{F}_5[x]$. It has no roots in $\mathbb{F}_5$, so is irreducible. But one construction of $\mathbb{F}_{25}$ is as $\mathbb{F}_5[y]/(y^2+2)$, and the element y in this field is a solution to $x^2 + 2 = 0$. Therefore $x^2 + 2$ is reducible over $\mathbb{F}_{25}$.

(b) The congruence classes are polynomials that differ by a multiple of $P(x)$. Using the division algorithm, any polynomial is seen to be congruent to a polynomial of degree less than d. All of these are obviously not congruent, as any multiple of $P(x)$ has too large degree to change one into another. Thus there are p^d such congruence classes, coming from choosing the d coefficients from $\mathbb{F}_p$.

(c) For details, see the book on page 97. The idea is pick an irreducible polynomial $P(x)$ of degree d over $\mathbb{F}_p$, then use $\mathbb{F}_p[x]/P(x)$.

(d) To show multiplicative inverses exist, use the Euclidean algorithm. Given a non-zero residue class, pick a polynomial $q(x) \in \mathbb{F}_p[x]$ representing it. Note that $q(x)$ and $P(x)$ are relatively prime. Then as with Euclidean algorithm in $\mathbb{Z}$, we can find solutions $r(x)$ and $t(x)$ such that

$$P(x)r(x) + q(x)t(x) = 1.$$

Looking at this modulo $P(x)$, we have a multiplicative inverese for $q(x)$.

(e) Consider x^3 and x in $\mathbb{F}_3[x]$. They are different polynomials, but define the same function as $\alpha^3 \equiv \alpha \pmod 3$ by Fermat's little theorem.

3. (a) Determine all irreducible polynomials in $\mathbb{F}_3[x]$ of degree 2 or less.

(b) Write down the addition and multiplication table for $\mathbb{F}_2[x]$ modulo $(x^2 + x + 1)$.

(c) The polynomials $P(x) = 1 + x + x^3$ and $Q(x) = 1 + x^2 + x^3$ are both irreducible in $\mathbb{F}_2[x]$. Since both have degree 3, we can identify the congruence classes of $\mathbb{F}_2[x]$ modulo $P(x)$ and the congruence classes of $\mathbb{F}_2[x]$ modulo $Q(x)$ with the eight polynomials $\mathbb{F}_2[x]$ of degree 2 or less (all possible remainders on division by a degree 3 polynomial). Show by example that the addition and multiplication rules for these small-degree polynomials are different in $\mathbb{F}_2[x]$ modulo $P(x)$ and $\mathbb{F}_2[x]$ modulo $Q(x)$. This is one reason it should be surprising that these two fields (and any two finite fields with the same number of elements) are "isomorphic", possibly after re-labeling the elements.

(d) Use the Euclidean algorithm (and polynomial division) to find a multiplicative inverse for $x + 1 \pmod{x^3 + x^2 + 1}$ in $\mathbb{F}_2[x]$.

Solution:

(a) Remember that a degree 2 polynomial will be irreducible if and only if it has no roots. So the degree two irreducible polynomials that are irreducible are x^2+1, $2x^2+2$, x^2+2x+2, $2x^2+x+1$, $x^2 + x + 2$ and $2x^2 + 2x + 1$ by running through and checking if 0, 1, or 2 are roots of each of the polynomials. All of the degree one polynomials are also irreducible because they can't be written as a product of two positive degree polynomials. Usually constant polynomials are not considered irreducible (for the same reason that -1 and 1 are not called primes – numbers with inverses are neither prime nor composite), but this is a point we did not emphasize in class, so either listing the constant polynomials or not is acceptable on this assignment.

(b) Representatives are $0, 1, x, x + 1$. The multiplication table is

	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

For example, $x^2 \equiv x^2 - (x^2 + x + 1) \equiv x + 1 \pmod 2$ because $x^2 + x + 1$ is zero.

(c) For example, in $\mathbb{F}_2[x]/P(x)$ we have $x^3 \equiv -x - 1$ and in $\mathbb{F}_2[x]/Q(X)$ we have $x^3 \equiv -x^2 - 1$. So the multiplication of x by x^2 gives different answers. Likewise, the addition of $x^3 + x$ and $2x$ gives different answers.

(d) We divide and see that $x^3 + x^2 + 1 = (x + 1)(x^2) + 1$, so a multiplicative inverse is x^2.

4. Let E be an elliptic curve defined over a field K. As usual, assume that 2 and 3 have multiplicative inverses in K.

(a) Explain why the addition law is *commutative*, that is, why $P+Q=Q+P$ for any points P, Q.

(b) Explain what it means to say that the addition law is *associative.* (This result is onerous to prove, and we will omit the proof.)

(c) Given a point $P \neq \infty$ on an elliptic curve, what is its negative $(-P)$? Use the equation for E to explain why $-P$ will always be a point on the elliptic curve (that is, why the curve must have reflectional symmetry in the x-axis).

(d) Give an algebraic description of the addition law (as on Page 362).

(e) Suppose that P and Q are two distinct points on an elliptic curve not equal to ∞. Let the line through P and Q intersect the curve in a third point R. Verify that the coordinates of $P+Q$, defined to be the reflection over the x-axis of R, are given by the formula you wrote down in the previous part. You may assume that $K=\mathbb{R}$ so you are comfortable with the geometry, but your solution (plus knowledge of algebraic geoemtry) will work in general.

Solution: The fact that 2 and 3 have multiplicative inverses means that the form of the group law given in class and the textbook is valid.

(a) The group law is defined such that $P+Q+R=\infty$ if P, Q, and R lie on the same line. The line through P and Q is independent of the ordering, so the group law is commutative. Alternately, note that the formulas given in the book don't change if we swap the points.

(b) To be commutative means for points P, Q, and R the way we group things doesn't matter: ie $(P+Q)+R=P+(Q+R)$. Without a better definition of the group law using more advanced algebraic geometry, this is painful to prove.

(c) Recall the negative is the reflection of P over the x-axis. If (x, y) satisfies $y^2=x^3+ax+b$, then so does $(x,-y)$, the reflection over the $x-$axis, because $(-y)^2=y^2$.

(d) See page 352.

(e) Let $P=(x_1, y_1)$ and $Q=(x_2, y_2)$. If $x_2=x_1$, the line through them is vertical. Then the geometric description of the group law tells us that the point at infinity is the third point of intersection of this line with the curve.

Letting $m=\frac{y_2-y_1}{x_2-x_1}$, we see an equation for the line through P and Q is $y=m(x-x_1)+y_1$. Substituting into the equation for the curve, we see

$$(m(x-x_1)+y_1)^2=m^2(x-x_1)^2+2m(x-x_1)y_1+y_1^2=x^3+ax+b.$$

Two of the solutions to this cubic in x are x_1 and x_2. We are interested in the third, x_3. The sum of the roots of a polynomial $t^3+r_2t^2+r_1t+r_0$ is $-r_2$, so we see that

$$x_1+x_2+x_3=m^2$$

(negative the the coefficient of x^2). Thus $x_3=m^2-x_2-x_1$. Substituting into the equation for the line gives

$$y_3=m(x_3-x_1)+y_1=m(x_3-x_1)+y_1.$$

The sum of P and Q is the reflection of (x_3, y_3) over the x-axis, ie $(x_3,-y_3)$.

Note that this derivation used nothing more than algebra, which means it will work over a finite field as well provided one interprets the geometry correctly.

5. Trappe–Washington Chapter 16 Exercise 2.

Solution: For each value of x, finding the values of y that solve the equation modulo 7, together with the point at infinity, gives the set of points on the curve: $\{(3,2),(3,5),(5,2),(5,5),(6,2),(6,5), \infty\}$. To add the points, use the formula or do geometry. The results are $(3,5)$ and $(5,2)$. Number theoristis use the computer algebra package SAGE to do calculations with elliptic curves, which is what I used to verify these calculations.

6. Trappe–Washington Chapter 16 Exercise 4.

   Solution: Given the point $P = (3, 5)$ on this elliptic curve, we can apply the group law to calculate $2P = P + P$, another rational point on the curve. This has coordinates $(\frac{129}{100}, \frac{-383}{1000})$.

7. Trappe–Washington Chapter 16 Exercise 15.

   Solution: If $k \equiv k' \pmod{2^n}$, then $kA = (k' + l2^n)A = k'A + l(2^nA) = k'A$.

   Now consider $T = 2^{n-1}A$. We know that $2T = 2^nA = \infty$ by definition. So any even multiple of T is ∞. If j is odd, then $jT = (j-1)T + T$. But $(j-1)T = \infty$, so $jT = T \neq \infty$.

   Writing $k = x_0 + \ldots + 2^{n-1}x_{n-1}$, we consider $B = kA$. Note that $2^{n-1}B = kT$, hence k is even ($x_0 = 0$) if and only if $2^{n-1}B = \infty$.

   For the last part, note that $2^{n-m-1}Q_m = 2^{n-m-1}(2^mx_m + \ldots 2^{n-1}x_{n-1})A$. This is $2^{n-1}x_mA$, because every larger term includes a 2^nA which is the identity element. The second part shows that x_m is even (0) if and only if $2^{n-m-1}Q_m = 2^{n-1}x_mA = \infty$.

   The following two bonus questions (which are very challenging) together prove our claim that every finite field can be realized by the construction described in Chapter 3.11.

8. **Bonus.** Prove that the number of elements in any finite field must be a prime power.

9. **Bonus.** Prove that any two finite fields with the same number of elements are isomorphic.

   Solution: See section 14.3 of Dummit and Foote or your favorite reference on abstract algebra.

   The following questions give applications of elliptic curves to cryptography.

10. **Bonus**.

    (a) Let $n = pq$. Explain how we can factor n by analyzing elliptic curves over $\mathbb{Z}/n\mathbb{Z}$.

    (b) Trappe–Washington Chapter 16 Exercise 6(a).

    Solution: The algorithm is discussed on page 356 of the textbook. For the problem, you can calculate $2P = (5, 16)$. Then $3P = 2P + P$ causes you to try to divide by the difference in the x-coordinates, which is $5 - 10$. This is not invertible modulo 30 because 5 and 30 share a common factor.

11. **Bonus.** Trappe-Washington Chapter 16 Exercise 9.

    Solution: If interested, you can read around Algorithm 7.3 of `http://math.arizona.edu/~mleslie/files/ecc.pdf`.