Groups, Fields, and Vector Spaces

Homework #2 (2010-2011), Answers

Q1. Extensions of finite fields

Recall that $\mathbb{Z}_2$ *is the field containing* $\{0,1\}$*, with addition and multiplication defined (mod 2). Consider the polynomial* $x^4+x+1=0$*. This has no solutions in* $\mathbb{Z}_2$*, so let's add a formal quantity* ξ *for which* $\xi^4+\xi+1=0$ *(and which satisfies the associative, commutative, and distributive laws for addition and multiplication with itself and with* $\{0,1\}$*), and see whether it generates a field.*

A. Using $\xi^4+\xi+1=0$*, express* ξ^r *in terms of 1,* ξ*,* ξ^2*, and* ξ^3 *for* $r=1,\ldots,15$*.*

Since field operations are "mod 2", we can replace -1 by +1, and 0 by 2. So, for example,
$\xi^4+\xi+1=0$ implies $\xi^4=\xi+1$. Using the field properties (distributive law),
$\xi^5=\xi\cdot\xi^4=\xi(\xi+1)=\xi^2+\xi$;
$\xi^6=\xi\cdot\xi^5=\xi(\xi^2+\xi)=\xi^3+\xi^2$;
$\xi^7=\xi\cdot\xi^6=\xi(\xi^3+\xi^2)=\xi^4+\xi^3=\xi^3+\xi+1$ (Here, we had to use $\xi^4=\xi+1$ in the last step.)

Working similarly, the table of coefficients is:

	ξ^3	ξ^2	ξ^1	ξ^0
$\xi^0=$	0	0	0	1
$\xi^1=$	0	0	1	0
$\xi^2=$	0	1	0	0
$\xi^3=$	1	0	0	0
$\xi^4=$	0	0	1	1
$\xi^5=$	0	1	1	0
$\xi^6=$	1	1	0	0
$\xi^7=$	1	0	1	1
$\xi^8=$	0	1	0	1
$\xi^9=$	1	0	1	0
$\xi^{10}=$	0	1	1	1
$\xi^{11}=$	1	1	1	0
$\xi^{12}=$	1	1	1	1
$\xi^{13}=$	1	1	0	1
$\xi^{14}=$	1	0	0	1
$\xi^{15}=$	0	0	0	1

Note that every combination of 0's and 1's occurs in some row, except for 0,0,0,0. (Why does this have to be?) Note also that $\xi^{15} = \xi^0 = 1$.

Comment 1: The constant term in the expansion of each ξ^r (i.e., the last column in the above table) is an "m-sequence," a sequence of 0's and 1's that (a) contains all quadruples of 0's and 1's exactly once, except for 0,0,0,0, and (b) is orthogonal (see later) to any shift of itself. This and other properties of m-sequences are neatly derived from the field properties. M-sequences are a kind of "shift register sequences", a term whose appropriateness should be apparent from the above construction.

Comment 2: The above comment applies to the coefficient of the ξ-term, the ξ^2-term, etc.

B. Using part A, show that the powers of ξ generate a field of size 16. This is $GF(2,4)$.

Since 0, 1, and ξ obey the associative, commutative, and distributive laws, we only have to show that these operations are closed under addition and multiplication, and that we can find multiplicative inverses for every element except 0.

To add two field elements ξ^a and ξ^b, we use the above table to represent each as a sum of 1, ξ, ξ^2, and ξ^3, add them, and convert back. For example, $\xi^4 + \xi^{13} = (\xi + 1) + (\xi^3 + \xi^2 + 1) = \xi^3 + \xi^2 + \xi = \xi^{11}$. To multiply two field elements ξ^a and ξ^b, we have $\xi^a \cdot \xi^b = \xi^{a+b}$; if the exponent $a+b$ exceeds 15, we note that $\xi^{a+b} = \xi^{a+b-15}$.

To find inverses, we note that $\xi^a \xi^{15-a} = \xi^{15} = \xi^0 = 1$.

C. Show that $\varphi(\xi) = \xi^2$ is an automorphism of $GF(2,4)$.

Two ways.

First, let $\eta = \xi^2$. We'll show that η satisfies the same equation as ξ, $x^4 + x + 1 = 0$. This means that η generates the same field as ξ. To show that $\eta^4 + \eta + 1 = 0$: $\eta^4 = (\xi^2)^4 = \xi^8$. So $\eta^4 + \eta + 1 = \xi^8 + \xi^2 + 1 = (\xi^2 + 1) + \xi^2 + 1 = 2\xi^2 + 2 = 0$, where we've used the table from part A at the second step, and the fact that we are adding mod 2 in the second step.

Better way:

This is a special case of something more general. In any extension field of $\{0,1\}$, the mapping $\varphi(z) = z^2$ is an automorphism. We need to check that addition and multiplication is preserved. For addition: $\varphi(z+w) = (z+w)^2 = z^2 + 2zw + w^2 = z^2 + w^2 = \varphi(z) + \varphi(w)$. For multiplication: $\varphi(zw) = (zw)^2 = zwzw = z^2 w^2 = \varphi(z)\varphi(w)$.

Comment: In fact, φ is an isomorphism.
$\varphi^2(z) = \varphi(\varphi(z)) = \varphi(z^2) = z^4$;
$\varphi^3(z) = \varphi(\varphi^2(z)) = \varphi(z^4) = z^8$;
$\varphi^4(z) = \varphi(\varphi^3(z)) = \varphi(z^8) = z^{16} = z$;
so $\varphi^{-1} = \varphi^3$. This also generalizes to GF(2,*n*).

Q2. Intrinsic relationships among dual spaces, etc.

A. Find an intrinsic relationship (a.k.a. "canonical homomorphism") between V and V^{**}*. (*V^{**} *is the dual of* V^**, i.e., the space of mappings from elements* φ *of* V^* *to the field.) That is, find a linear mapping* Φ *from elements v of V to elements* $\Phi(v)$ *of* V^{**}*.*

To define $\Phi(v)$, we need to display $\Phi(v)$ as a linear map from elements φ of V^* to a field element. That is, we need to specify the field element $[\Phi(v)](\varphi)$ that φ is mapped to by $\Phi(v)$. (and ensure that everything is linear). Since φ is in V^*, $\varphi(v)$ is a linear map from *V* to the field. So we choose $[\Phi(v)](\varphi) = \varphi(v)$.

B. Find an intrinsic relationship (a.k.a. "canonical homomorphism") between $Hom(V,W)$ *and* $Hom(W^*,V^*)$*. That is, find a linear mapping Z from elements* φ *of* $Hom(V,W)$ *to elements* $Z(\varphi)$ *of* $Hom(W^*,V^*)$*.*

To define $Z(\varphi)$, we need to display $Z(\varphi)$ as a linear map from elements ζ of W^* to elements $[Z(\varphi)](\zeta)$ in V^*. That is, we need to define how $[Z(\varphi)](\zeta)$ acts on an element *v* of *V*. Since φ is in $Hom(V,W)$, $\varphi(v)$ is in *W*, and ζ acts linearly on it. So it is natural to define $\left([Z(\varphi)](\zeta)\right)(v) = \zeta(\varphi(v))$. Everything is linear.

C. Find an intrinsic relationship (a.k.a. "canonical isomorphism") between $(V \otimes W)^*$ *and* $Hom(V,W^*)$*. That is, (a) given an element B of* $(V \otimes W)^*$*, find a linear mapping* Φ *that takes elements B of* $(V \otimes W)^*$ *to elements* $\Phi(B)$ *of* $Hom(V,W^*)$*. (b) Given an element* ξ *of* $Hom(V,W^*)$*, find a linear mapping* Ψ *that takes elements* ξ *of* $Hom(V,W^*)$ *to elements* $\Psi(\xi)$ *of* $(V \otimes W)^*$*. (c) Show that* Φ *and* Ψ *are inverses, i.e.,* $\Psi(\Phi(B)) = B$ *and* $\Phi(\Psi(\xi)) = \xi$*.*

(a) To define $\Phi(B)$, we have to show how it maps an element *v* of *V* into an element φ of W^*. That is, $[\Phi(B)](v)$ must be an element of W^*, i.e., a linear map from W to the scalars. SO we have to show how $[\Phi(B)](v)$ acts on an arbitrary *w* in *W* (and everything has to be linear). Since

B is given as an element of $(V\otimes W)^*$, it is a linear map from $v\otimes w$ to the field, just what we need. So $\Phi(B)$ is defined by $\left([\Phi(B)](v)\right)(w)=B(v\otimes w)$.

(b) To define $\Psi(\xi)$, we need to produce an element of $(V\otimes W)^*$, i.e., a linear map from tensors $v\otimes w$ to the field. Since ξ is in $Hom(V,W^*)$, $\xi(v)$ is in W^* and is therefore a map from *W* to the field, and $[\xi(v)](w)$ is linear in *v* and *w*. So we can take $([\Psi(\xi)](v\otimes w)=[\xi(v)](w)$.

(c) To show $\Psi(\Phi(B))=B$: $[\Psi(\Phi(B))](v\otimes w)=\left([\Phi(B)](v)\right)(w)=B(v\otimes w)$. (First equality is from (b), second is from (a)). To show $\Phi(\Psi(\xi))=\xi$:
$\left([\Phi(\Psi(\xi))](v)\right)(w)=(\Psi(\xi))(v\otimes w)=[\xi(v)](w)$. (First equality is from (a), second is from (b)).

Q3. Parity

A. What is the parity of a cyclic permutation of q elements, i.e., the permutation that puts 2 where 1 was, puts 3 where 2 was, puts 4 where 3 was, …, puts q where $q-1$ was, and puts 1 where q was?

This permutation can be generated by the following steps: swap 2 with 1, swap 3 with 1, swap 4 with 1, …, and swap *q* with 1. There are $q-1$ such steps, so the parity is $\left(-1\right)^{q-1}$.

In "permutation notation", this can be written $(123\ldots q)=(12)(13)(14)\ldots(1q)$, where $(abc\cdots ef)$ means "put *b* where *a* was, put *c* where *b* was, put *f* where *e* was, and put *a* where *f* was"

B. Recall the dihedral group: the symmetry group of a regular n-gon, containing rotations by $2\pi k/n$ radians, and reflections. (a) It can also be considered a permutation group, because it permutes the vertices of the n-gon. Which group elements correspond to a permutation with an even parity, and which to an odd parity? (b) The dihedral group can also be considered a permutation group in another way, because it acts on the edges of the n-gon. In this representation, which group elements correspond to permutations with even parity, and which ones to an odd parity?

(a) A rotation by $2\pi/n$ radians (one "step") is a cyclic permutation of the *n* vertices, and its parity (as in part A) is therefore $(-1)^{n-1}$. So a rotation by $2\pi k/n$ radians has parity $\left((-1)^{(n-1)}\right)^k=(-1)^{k(n-1)}$, since it is this same permutation applied *k* times.

The behavior of reflections depends on whether *n* is even or *n* is odd. If *n* is odd, then every reflection goes through one vertex, and the other $n-1$ vertices are swapped in pairs. So every reflection has a parity of $(-1)^{(n-1)/2}$. If *n* is even, then there are two kinds of reflections: those whose mirror planes go through the midpoints of opposite edges, and those whose mirror planes go through opposite vertices. The ones whose mirror planes go through the midpoints of opposite edges result in swapping the *n* vertices in pairs, and thus, have a parity of $(-1)^{n/2}$. The ones whose mirror planes go through opposite vertices leave those two vertices unchanged, and swap the remaining *n*-2 vertices in pairs. They therefore have a parity of $(-1)^{(n-2)/2}$.

(b) Rotations can be analyzed just as above; the one-step rotation is a cyclic permutation on the *n* edges.

For reflections: When *n* is odd, the analysis of part (a) holds, since one can track each edge by what happens to the opposite vertex. When *n* is even, the mirror planes that go through the midpoints of opposite edges have parity $(-1)^{(n-2)/2}$ (since they leave two edges unchanged), and the ones that go through opposite vertices have parity $(-1)^{n/2}$, since they swap all edges.

Comment:

This shows that parity is not an intrinsic property of the group element, only of how it is represented as a permutation group. (For *n* even, reflections have opposite parities, depending on whether they are considered to act on vertices or on edges.)

Also, it allows us to find some subgroups of the dihedral group: group elements that have even parity are the kernel of the mapping from the group to $\{+1,-1\}$ via the *parity* homomorphism.