Groups, Fields, and Vector Spaces

Homework #2 (2012-2013), Answers

Q1. Example homomorphisms.

A. Define the map $\varphi_n(x)$ from the integers $\mathbb{Z}$ to the set $\mathbb{Z}_n = \{0,...,n-1\}$ as the remainder of x, when divided by n. $\mathbb{Z}$ is a group under ordinary addition; $\mathbb{Z}_n$ is a group under addition "mod n" (i.e., $x \circ y$ is defined as the remainder of $x+y$ when divided by n). Is φ_n a homomorphism? If so, what is the kernel?

It is a homomorphism: we need to show that $\varphi_n(x)+\varphi_n(y)=\varphi_n(x+y)$, *i.e.*, that $\varphi_n(x)+\varphi_n(y)$ is the remainder of $x+y$ when divided by *n*.

Since $\varphi_n(x)$ is the remainder of *x* when divided by *n*, then $x = nX + \varphi_n(x)$ for some integer *X*. Similarly, $y = nY + \varphi_n(y)$ for some integer *Y*. Adding these two equations yields $x+y = n(X+Y)+\varphi_n(x)+\varphi_n(y)$, which shows that $\varphi_n(x)+\varphi_n(y)$ is the remainder of $x+y$ when divided by *n*.

The kernel is the set of integers in $\mathbb{Z}$ that map to the identity in $\mathbb{Z}_n$. That is, it is the set of integers that map to 0 in $\mathbb{Z}_n$, i.e., the set of integers that are multiples of *n*.

B. Consider the cyclic group with n elements, i.e., $C = \left\{e, r, r^2, ..., r^{n-1}\right\}$, with e the identity and r obeying $r^n = e$, and $n \ge 2$. (We can think of this group as being the rotations of the regular n-gon.) Show that $\phi_k(g) = g^k$ is a homomorphism. When is it "onto"? When is it an automorphism?

To show that $\phi_k(g) = g^k$ is a homomorphism, we need to show that $\phi_k(g_1)\phi_k(g_2) = \phi_k(g_1 g_2)$ for any two elements in *C*. Since $\phi_k(e) = e$, it suffices to show this for two elements that are not the identity. With $g_1 = r^u$ and $g_2 = r^v$, we have $\phi_k(r^u)\phi_k(r^v) = r^{uk} r^{vk} = r^{uk+vk} = r^{(u+v)k} = \phi_k(r^{u+v}) = \phi_k(r^u r^v)$.

ϕ_k is "onto" if every element r^t in *C* can be written in the form $\phi_k(r^u)$ for some *u*. It suffices to show this for $t=1$, since if $\phi_k(r^u) = r$ then $\phi_k(r^{ut}) = r^t$. To find a *u* for which $\phi_k(r^u) = r$ means to find a *u* for which $r^{ku} = r^1$, i.e., that ku and 1 differ by a multiple of *n*, i.e., that $ku - mn = 1$. By the Euclidean Algorithm, we are guaranteed this is possible when *k* and *n* are relatively prime. Conversely, if *k* and *n* have a common factor, say, $k = k'f$ and $n = n'f$, then $ku - mn$ also has a factor of *f*, and consequently, there is no *u* for which $r^{ku} = r^1$.

So ϕ_k is “onto” when *k* and *n* are relatively prime, and is not “onto” when they have a common factor. If ϕ_k is “onto”, then it is an automorphism, since its inverse is the ϕ_u defined above: $\phi_u(\phi_k(x)) = \phi_u(x^k) = x^{ku} = x^{1+mn} = x$.

(This is essentially the same argument used to show that $\mathbb{Z}_p$ is a field. If *n* is prime, then *k* and *n* cannot have a common factor, and all homomorphisms ϕ_k must be onto.)

C. Is the map $\varphi(j) = r^j$ from $\mathbb{Z}_n = \{0,...,n-1\}$ (with group operations defined in part A) to C, the cyclic group defined in part B, a homomorphism? Is it an isomorphism?

To see it is a homorphism: $\varphi(j_1)\varphi(j_2) = r^{j_1}r^{j_2} = r^{j_1+j_2} = \varphi(j_1 + j_2)$. It is obviously “onto”.

To see that it is an isomorphism, we need to find an inverse homomorphism from *C* to $\mathbb{Z}_n$. Define $\varphi'(r^j) = j$. It is a homomorphism, since $\varphi'(r^{j_1})\varphi'(r^{j_2}) = j_1 + j_2 = \varphi'(r^{j_1+j_2}) = \varphi'(r^{j_1}r^{j_2})$. φ and φ' are obviously inverses.

D. Homomorphisms involving the dihedral group. This is the group of rotations and reflections of the regular n-gon. Abstractly, it is $S = \left\{e, r, r^2, ..., r^{n-1}, a, ar, ar^2, ..., ar^{n-1}\right\}$, where e is the identity, r obeys $r^n = e$ and corresponds to a rotation, and a obeys $a^2 = e$ and corresponds to a reflection. a and r satisfy $ra = ar^{n-1}$.

Is $\rho(g) = g^2$ a homomorphism? If so, what is its kernel?

It is not a homomorphism, unless $n = 2$. $\rho(ar) = arar = a(ra)r = a(ar^{n-1})r = a^2r^n = ee = e$ but $\rho(a)\rho(r) = a^2r^2 = er^2 = r^2$. For $n = 2$, all of *S* is in the kernel.

E. Consider the map ψ from S (defined in D) to $P = \{-1, +1\}$, (where the group operation for P is multiplication), defined as follows: for $g = e$ or $g = r^k$, $\psi(g) = +1$. For $g = ar^k$ $(k = 1,...,n-1)$, $\psi(g) = -1$. Is ψ a hormormorphism from S to P? If so, what is its kernel?

We need to check whether $\psi(g_1)\psi(g_2) = \psi(g_1g_2)$. Each group element *g* is of the form r^j or ar^j.

Case 1: If the second term does not have an “*a*”, we can write $g_1 = a^ir^j$ and $g_2 = r^k$. This means that $\psi(g_2) = 1$ and also that $g_1g_2 = a^ir^jr^k = a^ir^{j+k}$, so $\psi(g_1g_2) = \psi(g_1)$, as needed for $\psi(g_1)\psi(g_2) = \psi(g_1g_2)$.

Case 2: If the second term has an “*a*”, we can write $g_1 = a^ir^j$ and $g_2 = ar^k$. This means that $\psi(g_2) = -1$ and also that $g_1g_2 = a^ir^jar^k = a^{i+1}r^{n-j+k}$ (see Homework 1). This means that g_1g_2

has an "*a*" only when g_1 does not have an "*a*" (*i*=0), and g_1g_2 does not have an "*a*" only when g_1 has an "*a*" (*i*=1). Either way, $\psi(g_1g_2)=-\psi(g_1)$, as needed for $\psi(g_1)\psi(g_2)=\psi(g_1g_2)$.

The kernel is the set of elements *g* of *S* for which $\psi(g)=1$, i.e., the elements of the form r^j (or *e*).

This shows that the cyclic group generated by *r* is a normal subgroup of the dihedral group.

Q2. 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* $r=1,...,15$.

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: $\varphi(zw) = (zw)^2 = zwzw = z^2 w^2 = \varphi(z)\varphi(w)$.