Groups, Fields, and Vector Spaces

Homework #2 (2012-2013)

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?

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?

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?

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?

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 homormorphism from *S* to *P*? If so, what is its kernel?

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 $r = 1,...,15$.
B. Using part A, show that the powers of ξ generate a field of size 16. This is $GF(2,4)$.
C. Show that $\varphi(\xi) = \xi^2$ is an automorphism of $GF(2,4)$.