Groups, Fields, and Vector Spaces

Homework #1 (2014-2015), Answers

Q1: Group or not a group?

Which of the following are groups? If a group, is it commutative? Finite or infinite? If infinite, is it discrete or continuous? If not a group, where does it fail?

A. The even integers $\{...-6,-4,-2,0,2,4,6...\}$ *, under multiplication*
Not a group. It fails to be a group because it doesn't contain the identity element

B. The set of all translations of 3-space, under composition
It's a commutative group; infinite; continuous

C. The set of all rotations of 3-space, under composition
It's a non-commutative group; infinite; continuous

D. The set of all $N \times N$ matrices with integer entries, under matrix addition
It's a commutative group, infinite, discrete

E. The set of all $N \times N$ matrices with integer entries, under matrix multiplication
Not a group. Some elements, for example, the matrix with all 0 entries, don't have inverses.

F. The set of all 2×2 *matrices with integer entries and determinant 1, under matrix multiplication*
It's a non-commutative group, infinite, discrete.

Q2. Modular arithmetic

For two integers x and y, we say $x = y$ *(mod k) if x and y differ by an integer multiple of k. So, for example, 3+4=2 (mod 5) and 6*9=10 (mod 11).*

A. Show that the integers $\{0,1,\ldots k-1\}$ *form a group under addition (mod k).*
Addition (mod *k*) inherits associativity and the identity element (0) from ordinary multiplication. To show that there's an additive inverse for an integer *x*, we note that $x+(k-x)=k$, so $x+(k-x)=0 \pmod{k}$, so $k-x$ is the additive inverse of *x*.

B. For what integers k do the integers $\{1,\ldots k-1\}$ *form a group under multiplication (mod k)?*
It is a group if, and only if, *k* is prime.

Multiplication (mod *k*) inherits associativity and the identity element (1) from ordinary multiplication. To determine whether there's a multiplicative inverse for an integer *x*, we seek another integer y for which $xy = 1$ (mod k). This means that $xy = 1 + ka$ for some integer a, or, that $xy - ka = 1$. But if x and k have a common factor greater than 1, say r, then $xy - ka$ also has r as a common factor, so $xy = 1$ (mod k) cannot be solved, and x does not have an inverse. This means that if k is not a prime, then $\{1,\ldots,k-1\}$ is not a group under multiplication (mod k).

Conversely, we can show that if k is a prime, then $\{1,\ldots,k-1\}$ is a group. One way to see this is as follows. Consider (for $1 \le x \le k-1$) all powers of x, $x^1, x^2, \ldots, x^q, \ldots$, and reduce each of them (mod k) to numbers $< k$. Since there are only a finite number of possibilities in $1 \le x \le k-1$, eventually there have to be repeats. If this repeat occurs for the integer exponents a and b ($a < b$), then $x^a = x^b$ (mod k). This in turn means that $x^a = x^b + Nk$ for some integer N. Since k is prime, x cannot divide k, and therefore x^a must divide N. So $1 = x^{b-a} + N'k$ for some integer N', i.e., $x^{b-a} = 1$ (mod k). This in turn means that x^{b-a-1} is the multiplicative inverse of x.

Q3. Normal subgroups

Definition: A subgroup H of G is said to be a "normal" subgroup if, for any element g of G and any element h of H, the combination ghg^{-1} is also a member of H.

A. Show that if φ is a homomorphism from G to some other group R, then the kernel of φ is a normal subgroup of G. (In class, we showed that the kernel must be a subgroup, here, show that it is normal as well.)

The kernel of φ is the set of all group elements h for which $\varphi(h) = e_R$. To show that the kernel is a normal subgroup, we need to show that if $\varphi(h) = e_R$, then $\varphi(ghg^{-1}) = e_R$, because the latter will mean that ghg^{-1} is in the kernel.

$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)e_R\varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e) = e_R$,
with the justification for the steps being: φ preserves structure; h is in the kernel; e_R is the identity in R, φ preserves structure; definition of inverses; φ preserves structure.

B. Show that if H is a normal subgroup and b is any element of G, then the right coset Hb is equal to the left coset, bH.

Say hb is a member of the right coset Hb. We want to show that it is equal to a quantity of the form bh' for some h' in H. To ensure that $bh' = hb$, we can choose $h' = b^{-1}hb$. Since H is assumed to be normal, $b^{-1}hb$ is in H, as required.

C. Show that if H is a normal subgroup, then any element of the right coset Hb , composed with any element of the right coset Hc, is a member of the right coset Hbc, with the product bc carried out according to the group operation in G.

Similar to B. We multiply a typical member of *Hb* by a typical member of *Hc*, and show it is in *Hbc*:
$(hb)(h'c) = hbh'c = hbh'b^{-1}bc = h''bc$, for $h'' = hbh'b^{-1}$. Note that h'' is guaranteed to be in *H*, since it is a product of two terms that are each in *H*: $h'' = h(bh'b^{-1})$.

D. Consider the mapping from group elements to cosets, $\varphi(b) = Hb$ *(where H is a normal subgroup). Show that this constitutes a homomorphism from the group G to the set of cosets, with the group operation on cosets defined by* $(Hb) \circ (Hc) = Hbc$.

First, we need to show that φ preserves structure. Using part C, $\varphi(b)\varphi(c) = HbHc = Hbc = \varphi(bc)$. Then, we need to find the identity element in the set of cosets. This is $H = He$, as can be seen from the fact that φ preserves structure. Then, we need to find the inverse of a coset Hb. This is Hb^{-1}, also from the fact that φ preserves structure.

E. Find the kernel of the homomorphism in D.

The kernel of φ is the set of elements of *G* that map onto the identity coset, $H = He$. If *b* is in this set, i.e., if $Hb = He$, then $hb = h'e$ for some *h* and h', so $b = h^{-1}h'$. So every element of the kernel is in *H*. The converse is equally easy; if *h* is in *H*, then the coset *Hh* is necessarily *H* itself.

Comment: The relationship between kernels, homomorphisms, and normal subgroups indicates how groups can be decomposed, and is a prototype for analogous statements about decomposing other algebraic structures.