Groups, Fields, and Vector Spaces

Homework #1 (2012-2013), 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 addition*
It's a commutative group; infinite; discrete

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

C. The set of all reflections of a sphere, under composition
Not a group, as it does not contain the identity. The composition of two reflections is NOT a reflection (it can't be—reflections invert handedness, so one reflection followed by a second reflection preserves handedness).

D. The set of all rotations and reflections of a sphere, under composition
It's a non-commutative group; infinite; continuous. Has two disconnected components – the component that preserves handedness (rotations, contains the identity) and the component that inverts handedness (reflections)

E. The set of all transformations T_p *defined by* $T_p(x) = x^p$*, under composition*
Not a group. It has an identity T_1 and obeys the associative law (since $T_p \circ T_q = T_{pq}$) but T_2 does not have an inverse.

F. The set of all reflections and rotations of a rectangle, under composition
It's a commutative group; finite. Four elements: the identity, one rotation (rotate in-plane by 180 deg), and two reflections (parallel to either pair of sides). Each element is its own inverse. Composing the two reflections yields the rotation; composing one reflection with the rotation yields the other reflection.

Q2. Dihedral groups (one step beyond cyclic groups)

The standard group operation is denoted by juxtaposition.

Consider the following distinct elements: e, a, and r. Assume that they compose in a way that obeys the associative law, that e is the identity, that a is of order 2, and that r is of order $n \geq 2$*. (Only* $n \geq 3$ *is interesting, though.) Suppose further that a and r satisfy* $ra = ar^{n-1}$*, and that the elements of the set* $S = \{e, r, r^2, ..., r^{n-1}, a, ar, ar^2, ..., ar^{n-1}\}$ *are all* *distinct. Show that this set constitutes a group, of size 2n. (This is known as the "dihedral group" D_n.)*

As a preliminary, we use $ra = ar^{n-1}$ to reduce $r^j a$ into something in the set *S*. First, $r^2 a = r(ra) = rar^{n-1} = ar^{n-1}r^{n-1} = ar^{2n-2} = ar^n r^{n-2} = ar^{n-2}$.
Continuing in this fashion, $r^j a = ar^{n-j}$. This will allow us to multiply any two elements in *S*.

Next, we need to show that when we apply the group composition law to two elements in *S*, the result remains in *S*. This breaks down into two cases, depending on whether the second term has an "*a*" factor:

Second term does not have an "*a*", i.e., $(a^i r^j)(r^k)$, for $i = 0$ or $i = 1$: If $j + k \le n - 1$, then $a^i r^j r^k = a^i r^{j+k}$, which is in *S*. If $j + k \ge n$, then $a^i r^j r^k = a^i r^{j+k} = a^i r^{j+k-n} r^n = a^i r^{j+k-n}$, which is also in *S*.

Second term does have an "*a*", i.e., $(a^i r^j)(ar^k)$, for $i = 0$ or $i = 1$: This is $a^i r^j ar^k = a^{i+1} r^{n-j} r^k$, which can be handled as in the previous case, noting that if $i = 1$, then $a^{i+1} = a^2 = e$.

G1 follows because each of the elements *e*, *a*, and *r* obey the associative rule.
G2 follows because *e* is in *S*.
To show G3: The inverse of *a* is *a* (since it is of order 2). The inverse of r^j is r^{n-j}, since $r^j r^{n-j} = r^n = e$. The inverse of ar^j is itself, since
$(ar^j)(ar^j) = a(r^j a)r^j = a(ar^{n-j})r^j = a^2 r^n = e$

Comment: This group is an abstract model for the rotations and reflections of regular *n*-gon. The elements ar^j, all of which are of order 2, correspond to reflections. The elements r^k correspond to rotations of $2\pi k / n$ radians.

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 will show that the kernel must be a subgroup, here, assume that it is, and 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, $\varphi(b) = Hb$. 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.