Groups, Fields, and Vector Spaces

Homework #2 (2008) for pages 4-9 of notes -- answers

Q1: Automorphisms. Let G = the group of real 2x2 matrices , nonzero determinant, under multiplication.

A. Consider the mapping T, defined by $T(M) = M^T$*, where* M^T *is the transpose of M (recall: the transpose exchanges rows and columns.) Is T an automorphism? What is* T^2*? Is it automorphism?*

T is not an automorphism, since $T(MN) = (MN)^T = N^T M^T = T(N)T(M)$ (the crucial step is the second equality: the transpose of a product of matrices is the product of the transpose in reverse order).

$T^2(M) = T(M^T) = (M^T)^T = M$, so T^2 is the identity transformation (and, trivially, an automorphism).

B. Consider the mapping V, defined by $V(M) = M^{-1}$*, where* M^{-1} *is the matrix inverse of M. Is V an automorphism? What is* V^2*? Is it an automorphism?*

V is not an automorphism, for exactly the same reason as in Q1A. (the crucial step is the second equality: the inverse of a product of matrices is the product of the inverses in reverse order). And, as in Q1A, V^2 is the identity transformation (and, trivially, an automorphism).

C. Consider $\psi = TV$*. Is* ψ *an automorphism? Is* ψ^2 *an automorphism?*
Combining Q1A and Q1B,
$\psi(MN) = TV(MN) = T(V(MN)) = T(V(N)V(M)) = TV(M)TV(N) = \psi(M)\psi(N)$
So, ψ is an automorphism. Since the automorphisms form a group, so is ψ^2. (Also, you can show that ψ^2 is the identity.)

D. An "inner" automorphism is an automorphism which can be written as $\varphi_A(M) = AMA^{-1}$*, for some A. Which of the above automorphisms are "inner"? Hint: recall a basic property of the determinant:* $\det(XY) = \det(X)\det(Y)$*. (That is, det is a homomorphism from G onto the reals, under multiplication.) Calculate* $\det(\varphi_A(M))$*. Calculate* $\det(\psi(M))$*.*
T and *V* are not automorphisms.
ψ is not "inner". For an inner automorphism φ_A,
$\det(\varphi_A(M)) = \det(AMA^{-1}) = \det(A)\det(M)\det(A^{-1}) = \det(A)\det(M)\left(\det(A)\right)^{-1} = \det(M)$.

But $\det(\psi(M)) \neq \det(M)$; take for example $M = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$, $\psi(M) = \begin{pmatrix} 1/a & 0 \\ 0 & 1/b \end{pmatrix}$, for which $\det M = ab$ and $\det(\psi(M)) = 1/(ab)$.

Q2: Centers. The "center" of a group G is the subset of elements α of G for $\alpha g = g\alpha$, for all group elements g. (For example, the center of a commutative group is the whole group.)

A. Show that the center of a group is a subgroup.
First, we need to show that if α and β is in the center, then so is $\alpha\beta$. Assume α and β commute with all of *G*. Then, $(\alpha\beta)g = \alpha(\beta g) = \alpha(g\beta) = (\alpha g)\beta = (g\alpha)\beta = g(\alpha\beta)$, which shows that $\alpha\beta$ commutes with all of *G*. Trivially, the identity for G commutes with all of G, so it serves as the identity for the center. Last, we need to show that if α is in the center, then so is α^{-1}. To see this: $\alpha^{-1}g = (g^{-1}\alpha)^{-1} = (\alpha g^{-1})^{-1} = g\alpha^{-1}$. (Middle equality because α commutes with every g^{-1}, other equalities because the inverse of a product is the product of the inverses in reverse order.

B. Show that the center is the kernel of the map from G into the inner automorphism group of G. That is, show that if α is in the center of G, then φ_α is the identity map on G, and conversely, that if φ_α is the identity map on G, then α is in the center of G.

$\varphi_\alpha(g) = \alpha g \alpha^{-1} = g\alpha\alpha^{-1} = g$, so φ_α is the identity automorphism.

C. Find the center of the group of 2x2 matrices in Q1.
Say $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in the center, and $g = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$.
$\alpha g = \begin{pmatrix} a & ax+b \\ c & cx+d \end{pmatrix}$ and $g\alpha = \begin{pmatrix} a+cx & b+dx \\ c & d \end{pmatrix}$, so $\alpha g = g\alpha$ for all *x* implies $c = 0$ and $a = d$.
Same idea for g^T yields $b = 0$. So α must be of the form $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Since this is a multiple of the identity, it commutes with all of *G*.

Q3. Finite fields.
Display the addition and multiplication tables for a finite field k with 4 elements.

Hint: Recall that the additive structure of k must be a group of size 4. There are two different ones: $\mathbb{Z}_4$ (the cyclic group of size 4), and $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, the direct sum of two groups of size 2. Show that the additive group cannot be $\mathbb{Z}_4$, by the following approach. From $1+1=2$, use the distributive law to show $2\times 2 = 0$, which cannot happen in a field – since this means that 2 has no multiplicative inverse. Then you only need to find a self-consistent multiplication table, to go along with the additive structure of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Carrying out the hint:
If the additive group is $\mathbb{Z}_4$, then $2\times 2 = (1+1)\times 2 = (1\times 2)+(1\times 2) = 2+2 = 0$. Then 2 would not have a multiplicative inverse. So the additive group cannot be $\mathbb{Z}_4$.

So the additive structure must be $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. We'll label the field elements 0 (the additive identity), 1 (the multiplicative identity), and two more abstract elements *x* and *y*. Since the additive structure is $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, $x + x = 0$ and similarly for *y*. So the addition table is

$+$	0	1	x	y
0	0	1	x	y
1	1	0	y	x
x	x	y	0	1
y	y	x	1	0

For multiplication: multiplication by 0 must yield 0. 1 is the multiplicative identity. Recall that the non-0 elements must form a group under multiplication. This is a group of size 3 ($\{1, x, y\}$), and the ONLY group of size 3 is the cyclic group (of rotations of a triangle), so it follows that $x \times x = y$.

Another way to see that we must have $x \times x = y$ is that, alternatively, if $x \times x = 1$, then $x \times y = x \times (x+1) = (x \times x) + (x \times 1) = 1 + x = y$, which would imply that *x* would be a "private" multiplicative identity for *y*, which is a contradiction.

So the multiplication table is

$\times$	0	1	x	y
0	0	0	0	0
1	0	1	x	y
x	0	x	y	1
y	0	y	1	x

Q4. (Bonus): How large is the automorphism group of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$? How large is the automorphism group of $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$? Are they commutative?

We can regard the group $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ as containing the elements {0,*a*,*b*,*c*}, with each of *a*, *b*, and *c* of order 2, and also, the product of any two different elements of {*a*,*b*,*c*} equaling the third element. That is, the three elements are all, abstractly, identical. So any permutation of them is an automorphism. There are 6 permutations on 3 elements. This is not commutative.

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$: There are 7 nonzero elements, and each is of order 2. Demonstrate that an automorphism ϕ can map one of these elements, say, *a*, either to itself, or to any of the other 7 elements. Having fixed $\phi(a)$, next show that ϕ can map any other element, say, *b*, to anything not equal to $\phi(a)$. With $\phi(a)$ and $\phi(b)$ fixed, then so is $\phi(ab)$. There are 4 elements whose fate is now determined: 0, *a*, *b*, and *ab*. Finally, show that ϕ can map one of the remaining elements, *c*, to anything that is not 0, $\phi(a)$, $\phi(b)$, or $\phi(ab)$. This determines ϕ, since the entire group consists of

0, *a*, *b*, *ab*, *c*, *ac*, *bc*, and *abc*. So there are 7 possibilities for *a*, 6 for *b*, and 4 for *c*, i.e. 168=7.6.4 automorphisms. It is not commutative (it contains the automorphism group of $\mathbb{Z}_2 \oplus \mathbb{Z}_2$).