Math 502: Abstract Algebra
Homework 2

Lawrence Tyler Rush
<me@tylerlogic.com>

January 5, 2014
http://coursework.tylerlogic.com/courses/upenn/math502/homework02

1

(a) The Heisenberg Group is a subgroup of the General Linear Group

First, because all elements of the real Heisenberg group are upper triangular, with one at each entry of the diagonal, then every element of $H(\mathbb{R})$ has determinant of one. Thus $H(\mathbb{R}) \subset \mathrm{GL}_3(\mathbb{R})$. Now for $x = y = z = 0$, the matrix of form

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$$

is the identity matrix. So the Heisenberg group contains the identity of $\mathrm{GL}_3(\mathbb{R})$. Because the right-hand side of

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x' & z' \\ 0 & 1 & y' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x + x' & z' + xy' + z \\ 0 & 1 & y' + y \\ 0 & 0 & 1 \end{pmatrix}$$

is in the format appropriate for $H(\mathbb{R})$, then $H(\mathbb{R})$ is closed under the group operation. Finally because

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -x & xy - z \\ 0 & 1 & -y \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & -x & xy - z \\ 0 & 1 & -y \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

then the inverse of

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$$

is

$$\begin{pmatrix} 1 & -x & xy - z \\ 0 & 1 & -y \\ 0 & 0 & 1 \end{pmatrix}$$

and because it is formatted in accordance with the definition of $H(\mathbb{R})$, then it is also contained in $H(\mathbb{R})$. Thus $H(\mathbb{R}) \subset \mathrm{GL}_3(\mathbb{R})$ contains the identity of $\mathrm{GL}_2(\mathbb{R})$, is closed under the group operation, and is closed under taking inverses, and therefore it is a subgroup of $\mathrm{GL}_3(\mathbb{R})$.

(b)

Let K be the subset of the Heisenberg Group defined by all matrices of the form

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Define $h : H(\mathbb{R}) \to \mathbb{R}$ by

$$h\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} = y$$

With this definition, since

$$h\left(\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & x' & z' \\ 0 & 1 & y' \\ 0 & 0 & 1 \end{pmatrix}\right) = h\begin{pmatrix} 1 & x+x' & z'+xy'+z \\ 0 & 1 & y+y' \\ 0 & 0 & 1 \end{pmatrix} = y+y' = h\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} h\begin{pmatrix} 1 & x' & z' \\ 0 & 1 & y' \\ 0 & 0 & 1 \end{pmatrix}$$

as well as

$$h\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 0$$

then h is a homomorphism, and moreover, since every element of the form

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and only elements of that form will map to 0, then K is the kernel of h. Hence K is a (normal) subgroup of $H(\mathbb{R})$.

Centralizer, $Z_{H(\mathbb{R})}(K)$, of K Since

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & x' & z' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x'+x & z'+z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & x' & z' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x'+x & x'y+z'+z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$$

then $z'+z = x'y+z'+z$, i.e. $x'y = 0$, must be true in order for the element

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$$

of $H(\mathbb{R})$ to be contained in the centralizer of K. Thus y must be zero, which implies that $Z_{H(\mathbb{R})}(K) = K$.

(c)

Since

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x' & z' \\ 0 & 1 & y' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+x' & z'+xy'+z \\ 0 & 1 & y'+y \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & x' & z' \\ 0 & 1 & y' \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x'+x & x'y+z'+z \\ 0 & 1 & y+y' \\ 0 & 0 & 1 \end{pmatrix}$$

then $\begin{pmatrix} 1 & x' & z' \\ 0 & 1 & y' \\ 0 & 0 & 1 \end{pmatrix}$ will commute with arbitrary $\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$ in $H(\mathbb{R})$ when $z + z' + xy' = z + z' + x'y$, i.e. when $xy' = x'y$. However, the only way for this to be possible independent of x and y is by having $x' = y' = 0$. So the center of the Heisenberg Group is the set of all matrices of the form $\begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

The center of the Heisenberg Group is isomorphic to $\mathbb{R}$ Define $\varphi : Z(H(\mathbb{R})) \to \mathbb{R}$ by

$$\varphi \begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = z$$

This mapping is a homomorphism between the group $Z(H(\mathbb{R}))$ and $\mathbb{R}$ over addition by the following

$$\varphi \left(\begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & z' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right) = \varphi \begin{pmatrix} 1 & 0 & z+z' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = z + z' = \varphi \begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + \varphi \begin{pmatrix} 1 & 0 & z' \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

By this construction, only the identity, I_3, will map to $0 \in \mathbb{R}$, and thus the kernel of φ is the trivial subgroup. Hence φ is injective. Finally, since for any $x \in \mathbb{R}$

$$\varphi \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = x$$

then φ is also surjective. Therefore $\varphi : Z(H(\mathbb{R})) \to \mathbb{R}$ is an injective and surjective homomorphism, i.e. $Z(H(\mathbb{R}))$ is isomorphic to $\mathbb{R}$.

(d) Extra Credit: Find all finite subgroups of $H(\mathbb{R})$

First, a helpful lemma.

Lemma 1.1. *For every element* $\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$ *of* $H(\mathbb{R})$*,*

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & nx & nz + \frac{n(n-1)}{2}xy \\ 0 & 1 & ny \\ 0 & 0 & 1 \end{pmatrix}$$

for $n \in \mathbb{Z}^+$*.*

Proof. As a base case, we see that when $n = 1$, the formula holds:

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}^1 = \begin{pmatrix} 1 & x & z + \frac{0}{2}xy \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$$

So assume that the formula holds for $m - 1 > 1$. Then we have that

$$\begin{aligned}
\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}^m &= \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}^{m-1} \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & (m-1)x & (m-1)z + \frac{(m-1)(m-2)}{2}xy \\ 0 & 1 & (m-1)y \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & mx & (m-1)z + \frac{(m-1)(m-2)}{2}xy + (m-1)xy + z \\ 0 & 1 & my \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & mx & \frac{(m-1)(m-2)+2(m-1)}{2}xy + mz \\ 0 & 1 & my \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & mx & \frac{m(m-1)}{2}xy + mz \\ 0 & 1 & my \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}$$

Hence through use of the inductive hypothesis we see the formula holds for m as well. □

For every element $h = \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$ of $H(\mathbb{R})$, Lemma 1.1 informs us that if x or y is nonzero, then h can generate an infinite number of elements. Therefore in order for h to be contained within a finite subgroup of $H(\mathbb{R})$, x and y must be zero. However, in that case Lemma 1.1 tells us that

$$\begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & 0 & nz \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

which implies that z must also be zero in order to be contained in a finite subgroup of $H(\mathbb{R})$. This leaves us with the identity element being the sole element of $H(\mathbb{R})$ that can be contained in a finite subgroup. Hence

$$\left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

is the only finite subgroup of $H(\mathbb{R})$

2 The Quaternion Group Q

(a) Find all subgroups of Q

Since Q has eight elements, then the order of the subgroups must be either 1, 2, 4, or 8. The following shows the subgroups obtained from the generators of the individual elements of Q:

$$\begin{aligned}
\langle 1\rangle &= \{1\}\\
\langle -1\rangle &= \{-1,1\}\\
\langle i\rangle &= \{i,-1,-i,1\}\\
\langle -i\rangle &= \{-i,-1,i,1\}\\
\langle j\rangle &= \{j,-1,-j,1\}\\
\langle -j\rangle &= \{-j,-1,j,1\}\\
\langle k\rangle &= \{k,-1,-k,1\}\\
\langle -k\rangle &= \{-k,-1,k,1\}
\end{aligned}$$

which yields the five subgroups $\{1\}$, $\{-1,1\}$, $\{1,i,-1,-i\}$, $\{1,j,-1,-j\}$, and $\{1,k,-1,-k\}$. Based on this, we can see that the subgroup generated by any two elements will result in one of the above subgroups (when one of the two elements is 1 or -1), or a subset of at least 6 elements (when the two are of $i, j, k, -i, -j,$, or $-k$), which must be the subgroup Q as 6 is not a divisor of $\#Q = 8$. Hence the only subgroups of Q are:

$$\{1\}, \{-1,1\}, \{1,i,-1,-i\}, \{1,j,-1,-j\}, \{1,k,-1,-k\}, Q$$

(b) Which subgroup above is the center

Because i, j, k are anticommutative with respect to each other, then the center cannot contain any one of those three elements. Based on the subgroups above, this leaves $\{1\}$ and $\{1,-1\}$, however, Q is a p-group since its order is $8 = 2^3$, which implies the non-trivality of the center. Hence $Z(Q) = \{1,-1\}$.

(c) Is Q isomorphic to D_8

The quaternion group Q is not isomorphic to D_8. Letting r be the rotational symmetry element in D_8 and s the mirror symmetry which generate the group, then both r^2 and s are distinct elements with order two, implying that there are two distinct subgroups with order two. This, however, conflicts with the previous part of the problem in which we saw that Q only has a single subgroup of order two.

(d) Extra Credit

3

(a) Explicitly determine the conjugacy classes of $\mathrm{GL}_2(\mathbb{C})$

Because two matrices $A, B \in \mathrm{GL}_2(\mathbb{C})$ will be in the same conjugacy class if there is a $P \in \mathrm{GL}_2(\mathbb{C})$ such that $PAP^{-1} = B$, then we can see that the conjugacy classes of $\mathrm{GL}_2(\mathbb{C})$ are simply the equivalence classes of the similarity relation. Thus we can use the Jordan Canonical Form to aide in our classification.

Now because $\mathbb{C}$ is algebraically closed, Theorem 23 [DF04, pg. 493] (repeated in Theorem A.1 for convenience) informs us that every element of $\mathrm{GL}_2(\mathbb{C})$ will be similar to either

$$\begin{pmatrix} \lambda & 1 \\ & \lambda \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \lambda_1 & \\ & \lambda_2 \end{pmatrix}$$

for $\lambda, \lambda_1, \lambda_2 \in \mathbb{C}^\times$, and uniquely so up to permutation of λ_1 and λ_2. Hence by defining S as

$$S = \left\{ \begin{pmatrix} \lambda & 1 \\ & \lambda \end{pmatrix} \,\middle|\, \lambda \in \mathbb{C}^\times \right\} \bigcup \left\{ \begin{pmatrix} a+bi & \\ & c+di \end{pmatrix} \,\middle|\, a+bi, c+di \in \mathbb{C}^\times \text{ and } \big(a < c \text{ or } (a = c \text{ and } b \leq d)\big) \right\}$$

where the goofy-looking condition on the right side is in place so that S doesn't contain both $\begin{pmatrix} \lambda_1 & \\ & \lambda_2 \end{pmatrix}$ and $\begin{pmatrix} \lambda_2 & \\ & \lambda_1 \end{pmatrix}$, we get that $S \subset \mathrm{GL}_2(\mathbb{C})$ such that every matrix of $\mathrm{GL}_2(\mathbb{C})$ is a conjugate to a unique element of S.

(b) Extra Credit: Explicitly determine the conjugacy classes of $SL_2(\mathbb{C})$

Because the conjugacy classes of $\mathrm{GL}_2(\mathbb{C})$ are the equivalence classes of the similarity relation and similar matrices have the same determinant, then then $S_1 = \{A \in S \mid \det(A) = 1\}$ (where S is as above) will be a subset of $\mathrm{SL}_2(\mathbb{C})$ for which every element of the $\mathrm{SL}_2(\mathbb{C})$ will be conjugate to a unique element of S_1.

4

Denote, by P_n, the boundary of the regular n-gon centered at the origin of $\mathbb{R}^2$. We will follow the lead of [DF04] here and let s be the reflection symmetry and r being the rotational symmetry that generate D_{2n}. Also denote the line across which s reflects by ℓ_s.

(a) What is the average number of fixed points in P_n for a random element in D_{2n}

The identity element certainly fixes all the points of P_n. The rotational elements of D_{2n}, r, r^2,…, r^{n-1}, will not fix any points since they simply rotate P_n. And finally, the elements s, sr, sr^2,…, sr^{n-1} will each fix two points since sr^i will first rotate by ${}^{2\pi i}\!/_{n}$ radians and then reflect across ℓ_s, meaning that any point that is ${}^{\pi i}\!/_{n}$ off of ℓ_s from the origin (in the direction opposite that of the direction of rotation) will be reflected back to it's original position after being acted on by sr^i. There are two such points for each sr^i; one ${}^{\pi i}\!/_{n}$ radians off of each of the two points at which ℓ_s and P_n intersect. Hence, letting $f : D_{2n} \to P_n$ be $f(x) = \{p \in P_n \mid x \text{ fixes } p\}$, we get the following number of expected fixed points for a randomly chosen element in D_{2n}

$$\frac{1}{2n}\left(|f(r^0)| + \sum_{i=1}^{n-1} |f(r^i)| + \sum_{i=0}^{n-1} |f(sr^i)|\right) = \frac{1}{2n}\left(|P_n| + \sum_{i=1}^{n-1} 0 + \sum_{i=0}^{n-1} 2\right) = \frac{|P_n| + 2n}{2n}$$

(b) Extra Credit: What is the average size of $\mathrm{Stab}_{D_{2n}}(y)$ for a random element $y \in P_n$

Again except for the identity fixing all $|P_n|$ points, the rotations of D_{2n} will not fix any points, and every sr^i will fix two points as per the previous part of the problem. This implies that $|\mathrm{Stab}_{D_{2n}}(y)| = 1$ for all y which are not fixed by some sr^i and $|\mathrm{Stab}_{D_{2n}}(y)| = 2$ for all y which are fixed by some sr^i. However there are only a finite number of the latter and uncountably many of the former, resulting in the average size of 1.

5

(a) Determine explicitly the group $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$

Any element of $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$ will map the identity element to itself because it is a homomorphism. Therefore, since $\mathbb{Z}/5\mathbb{Z}$ is cyclic, any automorphism will simply permute the non-identity elements. Hence if we denote $\mathbb{Z}/5\mathbb{Z}$ by $\langle a\rangle$ for clarity, then for any $\varphi \in \mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$, $\varphi(a) = a^i$ for some $i \in \{1, 2, 3, 4\}$. However, because φ is a homomorphism, this completely dictates the mapping by φ of a^2, a^3, and a^4, i.e.

$$\begin{aligned}\varphi(a^2) &= (\varphi(a))^2 = a^{2i}\\ \varphi(a^3) &= (\varphi(a))^3 = a^{3i}\\ \varphi(a^4) &= (\varphi(a))^4 = a^{4i}\end{aligned}$$

Hence, by defining φ_i to be the automorphism of $\mathbb{Z}/5\mathbb{Z}$ that maps a to a^i, we can then see that $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}) = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}$.

(b) Is $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$ cyclic?

The group $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$ is a cyclic group with generator φ_2 where φ_2 is as per above. Since each automorphism of $\mathbb{Z}/5\mathbb{Z}$ is defined by it's image of a, then the following

$$\begin{aligned}\varphi_1(a) = {}& a && = \varphi_2(\varphi_2(\varphi_2(\varphi_2(a))))\\ \varphi_2(a) = {}& a^2 && = \varphi_2(a)\\ \varphi_3(a) = {}& a^3 && = \varphi_2(\varphi_2(\varphi_2(a)))\\ \varphi_4(a) = {}& a^4 && = \varphi_2(\varphi_2(a))\end{aligned}$$

reveals that φ_2 generates $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z})$.

(c) Extra Credit: Determine $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ for $n \geq 2$

Since the $\mathbb{Z}/n\mathbb{Z}$ is cyclic, the argument above still applies, but just more generally; that is that each automorphism is a permutation of the non-identity elements and is completely defined by its mapping of a. So because a can be mapped to $a, a^2, \ldots, a^{n-1}$ then $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = \{\varphi_1, \varphi_2, \ldots, \varphi_{n-1}\}$ where φ_i is defined as above.

References

[DF04] D.S. Dummit and R.M. Foote. *Abstract Algebra.* John Wiley & Sons Canada, Limited, 2004.

A Theorems Repeated from Other Sources

Theorem 23 of Chapter 12 of [DF04, pg. 493]:

Theorem A.1 (Jordan Canonical Form for Matrices)**.** *Let A be an $n \times n$ matrix over the field F and assume F contains all the eigenvalues of A.*

1. *The matrix of A is similar to a matrix in Jordan canonical form, i.e. there is an invertible $n \times n$ matrix P over F such that $P^{-1}AP$ is a block diagonal matrix whose diagonal blocks are the Jordan blocks for the elementary divisors of A.*
2. *The Jordan canonical form for A is unique up to a permutation of the Jordan blocks along the diagonal.*