Math 502: Abstract Algebra
Homework 3

Lawrence Tyler Rush
<me@tylerlogic.com>

January 5, 2014
http://coursework.tylerlogic.com/courses/upenn/math502/homework03

1

(a) Show that $(\mathbb{Z}/n\mathbb{Z})^\times$ is isomorphic to $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$.

Any element of $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ will map the identity element to itself because it is a homomorphism. Therefore, since $\mathbb{Z}/n\mathbb{Z}$ is cyclic, any automorphism will simply permute the non-identity elements. Hence for any $\varphi \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$, $\varphi(\overline{1}) = \overline{i(1)} = \overline{i}$ for some $i \in \{1, 2, \ldots, n\}$. However, because φ is a homomorphism, this completely dictates the mapping by φ of $\overline{2}$, $\overline{3}$,... $\overline{n}$, i.e.

$$\begin{aligned}
\varphi(\overline{2}) &= \left(\varphi(\overline{1})\right)^2 = \overline{2i} \\
\varphi(\overline{3}) &= \left(\varphi(\overline{1})\right)^3 = \overline{3i} \\
&\vdots \\
\varphi(\overline{n}) &= \left(\varphi(\overline{1})\right)^n = \overline{ni}
\end{aligned}$$

Hence, by defining φ_i to be the automorphism of $\mathbb{Z}/n\mathbb{Z}$ that maps $\overline{1}$ to $\overline{i}$, we can then see that

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = \{\varphi_i |\, \gcd(i, n) = 1\}$$

Note that we need the stipulation of i, n being coprime because if j is not coprime to n, then we would be able to find a $0 < k < n$ such that $kj = n$, i.e. $\overline{j}$ wouldn't generate the group, and therefore φ_j would not be a bijection.

Since $(\mathbb{Z}/n\mathbb{Z})^\times$ are the units of $\mathbb{Z}/n\mathbb{Z}$, i.e. the equivalence classes of all the coprime numbers between 0 and n, then the above implies that this is in one-to-one correspondence with $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$. The bijection is $\phi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ defined by

$$\overline{i} \mapsto \varphi_i$$

(b) Is $(\mathbb{Z}/5\mathbb{Z})^\times$ a cyclic group?

Yes it is cyclic; it is $\langle\overline{2}\rangle$.

$$\begin{aligned}
\overline{2}^0 &= 1 \bmod 25 \\
\overline{2}^1 &= 2 \bmod 25 \\
\overline{2}^2 &= 4 \bmod 25 \\
\overline{2}^3 &= 3 \bmod 25
\end{aligned}$$

(c) Extra Credit: Is $(\mathbb{Z}/25\mathbb{Z})^\times$ a cyclic group?

Yes it is cyclic; it is $\langle\overline{2}\rangle$, since 5, 10, 15, and 20 are all coprime to 25 (and therefore their equivalence classes are not in $(\mathbb{Z}/25\mathbb{Z})^\times$

$$\begin{aligned}
\overline{2}^0 &= 1 \bmod 25 \\
\overline{2}^1 &= 2 \bmod 25 \\
\overline{2}^2 &= 4 \bmod 25 \\
\overline{2}^3 &= 8 \bmod 25 \\
\overline{2}^4 &= 16 \bmod 25 \\
\overline{2}^5 &= 7 \bmod 25 \\
\overline{2}^6 &= 14 \bmod 25 \\
\overline{2}^7 &= 3 \bmod 25 \\
\overline{2}^8 &= 6 \bmod 25 \\
\overline{2}^9 &= 12 \bmod 25 \\
\overline{2}^{10} &= 24 \bmod 25 \\
\overline{2}^{11} &= 23 \bmod 25 \\
\overline{2}^{12} &= 21 \bmod 25 \\
\overline{2}^{13} &= 17 \bmod 25 \\
\overline{2}^{14} &= 9 \bmod 25 \\
\overline{2}^{15} &= 18 \bmod 25 \\
\overline{2}^{16} &= 11 \bmod 25 \\
\overline{2}^{17} &= 22 \bmod 25 \\
\overline{2}^{18} &= 19 \bmod 25 \\
\overline{2}^{19} &= 13 \bmod 25
\end{aligned}$$

(d) Extra Credit

2

Let T be the set of diagonal matrices in $\mathrm{GL}_2(\mathbb{R})$.

(a) Centralizer of T in $\mathrm{GL}_n(\mathbb{R})$

For $n = 2$ Because of the following

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x & \\ & y \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} ax & by \\ cx & dy \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad-bc}\begin{pmatrix} adx - bcy & ab(y-x) \\ cd(x-y) & -bcx + ady \end{pmatrix}$$

we know that for the above to be equal to $\begin{pmatrix} x & \\ & y \end{pmatrix}$, because the determinant $ad - bc$ needs to be non-zero, that a and d need to both be zero and $bc = -1$, or b and c need to both be zero and $ad = 1$. Hence,

$$Z_{\mathrm{GL}_2(\mathbb{R})}(T) = \left\{ \begin{pmatrix} a & \\ & 1/a \end{pmatrix} \middle| a \neq 0 \right\} \bigcup \left\{ \begin{pmatrix} & b \\ -1/b & \end{pmatrix} \middle| b \neq 0 \right\}$$

For $n = 3$

(b) Normalizer of T in $\mathrm{GL}_n(\mathbb{R})$

For $n = 2$ For the following to be in T,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & \\ & y \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} ax & by \\ cx & dy \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad-bc} \begin{pmatrix} adx - bcy & ab(y-x) \\ cd(x-y) & -bcx + ady \end{pmatrix}$$

either a and d need to both be zero, or b and c need to both be zero, but exclusively so because the determinant, $ad - bc$, needs to be nonzero. Hence we have that

$$N_{\mathrm{GL}_2(\mathbb{R})}(T) = \left\{ \begin{pmatrix} a & b \\ b & d \end{pmatrix} \middle| b = c = 0 \text{ or } a = d = 0 \right\}$$

For $n = 3$

(c) Extra Credit

(d) Extra Credit

3

(a)

(b) Extra Credit

(c) Extra Credit

---

4 Classify all groups G where $\mathrm{Aut}(G) = \{id_G\}$

Such a G must be abelian If G were not abelian, then there would be at least one non-identity element, g, outside of the center of G. The map $\sigma_g : G \to G$ defined by $\sigma_g(h) = ghg^{-1}$, i.e. conjugation by g, would then be an automorphism of G since there must exist at least one $h \in G$ such that $ghg^{-1} \neq h$ as $g \notin Z(G)$. Hence σ_g is a non-identity map contained in $\mathrm{Aut}(G)$.

5

(a) The trivial subspace and $\mathbb{R}^2$ are the only subspaces closed under left action by $\mathrm{GL}_2(\mathbb{R})$

It's clear that the trivial subspace and $\mathbb{R}^2$ are both closed subspaces under action by $\mathrm{GL}_2(\mathbb{R})$. The only other subspaces of $\mathbb{R}^2$ are 1-dimensional, i.e. lines of $\mathbb{R}^2$. So simply a rotation, by say π, like

$$\begin{pmatrix} \cos\pi & -\sin\pi \\ \sin\pi & \cos\pi \end{pmatrix}$$

will take a vector in a 1-dimensional subspace outside of the subspace.

(b)

Functions are stable under action of the identity element. The first property of an action is satisfied by the following

$$\begin{pmatrix} 1 & \\ & 1 \end{pmatrix} \cdot f(x,y) = f(1x + 0y, 0x + 1y) = f(x,y)$$

The "associative" property of an action. Let $A, B \in \mathrm{GL}_2(\mathbb{R})$ with

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} m & n \\ q & r \end{pmatrix}$$

Because this

$$\begin{aligned}
A \cdot B \cdot f(x,y) &= A \cdot \begin{pmatrix} m & n \\ q & r \end{pmatrix} \cdot f(x,y) \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot f(mx+qy, nx+ry) \\
&= f(m(ax+cy) + q(bx+dy), n(ax+cy) + r(bx+dy)) \\
&= f\big((ma+qb)x + (mc+qd)y, (na+rb)x + (nc+rd)y\big)
\end{aligned}$$

is the same as

$$\begin{aligned}
(AB) \cdot f(x,y) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} m & n \\ q & r \end{pmatrix} \cdot f(x,y) \\
&= \begin{pmatrix} am+bq & an+br \\ cm+dq & cn+dr \end{pmatrix} \cdot f(x,y) \\
&= f\big((am+bq)x + (cm+dq)y, (an+br)x + (cn+dr)y\big) \\
&= f\big((am+qb)x + (mc+qd)y, (na+rb)x + (nc+rd)y\big)
\end{aligned}$$

then the "associative" property of an action holds for this action.

(c) Extra Credit

---

6 Is "is a normal subgroup" a transitive relation?

The "normality" relation is not transitive. In the group $D_{2(8)} = D_{16}$, we have $\langle s, r^2 \rangle \trianglelefteq D_{16}$ and $\langle s, r^4 \rangle \trianglelefteq \langle s, r^2 \rangle$, however, $\langle s, r^4 \rangle \not\trianglelefteq D_{16}$.

The subgroup $\langle s, r^2 \rangle$ is normal in D_{16} by

$$(s^k r^j)(s^\ell r^{2i})(s^k r^j)^{-1} = s^k r^j s^\ell r^{2i} r^{-j} s^k = s^k s^\ell r^{-j} r^{2i} r^{-j} s^k = s^{k+\ell} r^{2(i-j)} s^k = s^{2k+\ell} r^{2(j-i)} = s^\ell r^{2(j-i)} \in \langle s, r^2 \rangle$$

and $\langle s, r^4 \rangle$ is normal in $\langle s, r^2 \rangle$ by

$$(s^k r^{2j})(s^\ell r^{4i})(s^k r^{2j})^{-1} = s^k r^{2j} s^\ell r^{4i} r^{-2j} s^k = s^{k+\ell} r^{-2j} r^{4i} r^{-2j} s^k = s^{k+\ell} r^{4(i-j)} s^k = s^{2k+\ell} r^{4(j-i)} = s^\ell r^{4(j-i)} \in \langle s, r^4 \rangle$$

but the following demonstrates that $\langle s, r^4 \rangle \ntrianglelefteq D_{16}$

$$r(sr^4)r^{-1} = rsr^3 = sr^{-1}r^3 = sr^2 \notin \langle s, r^4 \rangle$$

References