Name:

Abstract Algebra (Math 3063)
Midterm Exam II - Solutions

PROFESSOR PAUL BAILEY
FRIDAY, APRIL 12, 2009

Problem 1. Let p be a positive odd integer.

(a) How many p-cycles are in A_p?

(b) How many distinct cyclic subgroups of order p are in A_p?

Solutions. Since p is odd, every p-cycle is an even permutation, so every p-cycle in S_p is in A_p. Thus, we count p-cycles in S_p.

Every p-cycle involves every positive integer from 1 to p; (that is, n is in its support for $n = 1, \dots, p$). So, we may assume that the cycle is written with its first position equalling 1. The remaining $p-1$ positions can be anything, and we will obtain a different cycle for each arrangement of 2 through p placed in these positions; there are $(p-1)!$ such arrangements, and so there are $(p-1)!$ p-cycles in S_p.

Each cyclic subgroup of order p contains a unique p-cycle which sends 1 to 2, and we may write such an element with 1 and 2 in the first two positions of the cycle. The remaining $p-2$ positions can be anything, and each arrangement of 3 through p in the remaining $p-2$ positions creates a different cyclic subgroup. There are $(p-2)!$ such arrangements, and so there are $(p-2)!$ cyclic subgroups of order p in S_p. □

Problem 2. Let p be a positive prime integer and define

$$\phi : \mathbb{Z}_p \to \mathbb{Z}_p \quad \text{by } \phi(a) = a^p.$$

(a) Show that ϕ is bijective.

(b) Show that $\phi(ab) = \phi(a)\phi(b)$.

(c) Show that $\phi(a+b) = \phi(a) + \phi(b)$ (hint: use the binomial theorem).

Solution. First we show that ϕ is injective. Let $a, b \in \mathbb{Z}_p$ such that $a^p = b^p$. If $a = 0$, then $a^p = 0$, so $b^p = 0$, and since $\mathbb{Z}_p$ contains no zero-divisors, $b = 0$; similarly, $b = 0$ implies $a = 0$. Otherwise, we have $a, b \in \mathbb{Z}_p^*$, and by Fermat's Little Theorem, $a^p = a$ and $b^p = b$. Thus $a = a^p = b^p = b$, so ϕ is injective.

Since ϕ is an injective function from a finite set to itself, it is necessarily surjective; thus ϕ is bijective.

Since multiplication is commutative in $\mathbb{Z}_p$, we have

$$\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b).$$

Finally, recall the binomial theorem:

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}.$$

Now p divides $\binom{p}{k}$ for $0 < k < p$, so these terms of the sum equal zero in $\mathbb{Z}_p$; thus

$$\phi(a+b) = (a+b)^p = a^0 b^p + a^p b^0 = a^p + b^p = \phi(a) + \phi(b).$$

□

Problem 3. Let G be a group and let $H = \{h \in G \mid h = g^2 \text{ for some } g \in G\}$. Suppose that $H \leq G$.

(a) Show that $H \triangleleft G$.

(b) Show that G/H is abelian.

Solution. Let $h \in H$ and $g \in G$. Then $h = x^2$ for some $x \in G$, and

$$g^{-1}hg = g^{-1}x^2g = g^{-1}x(gg^{-1})xg = (g^{-1}xg)(g^{-1}xg) = (g^{-1}xg)^2.$$

The latter expression is clearly a member of H, since it is the square of an element of G. Thus $g^{-1}HG \subset H$, which implies that $H \triangleleft G$.

We have previously seen that if the square of every element in a group is trivial, then the group is abelian. Let $g \in G$, so that $\overline{g} = gH$ is an arbitrary member of G/H. Then $g^2 \in H$, so $\overline{g}^2 = \overline{g^2} = H = \overline{1}$; thus G/H is abelian. $\square$

Problem 4. Consider the groups $\mathbb{R}$ under addition and $\mathbf{GL}_2(\mathbb{R})$ under matrix multiplication. Let

$$M = \left\{ A \in \mathbf{SL}_2(\mathbb{R}) \mid A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \right\}.$$

(a) Show that $\phi : \mathbb{R} \to \mathbf{GL}_2(\mathbb{R})$ given by $\phi(x) = \begin{bmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{bmatrix}$ is a group homomorphism.

(b) Show that $\phi(\mathbb{R}) = M$.

(c) Conclude that $M \leq \mathbf{SL}_2(\mathbb{R})$ and that $M \cong \mathbb{R}/2\pi\mathbb{Z}$.

Solution. Let $x_1, x_2 \in \mathbb{R}$. Then

$$\begin{aligned}
\phi(x_1)\phi(x_2) &= \begin{bmatrix} \cos x_1 & -\sin x_1 \\ \sin x_1 & \cos x_1 \end{bmatrix} \begin{bmatrix} \cos x_2 & -\sin x_2 \\ \sin x_2 & \cos x_2 \end{bmatrix} \\
&= \begin{bmatrix} \cos x_1 \cos x_2 - \sin x_1 \sin x_2 & \cos x_1 \sin x_2 + \sin x_1 \cos x_2 \\ -\sin x_1 \cos x_2 - \cos x_1 \sin x_2) & -\sin x_1 \sin x_2 + \cos x_1 \cos x_2 \end{bmatrix} \\
&= \begin{bmatrix} \cos x_1 \cos x_2 - \sin x_1 \sin x_2 & \cos x_1 \sin x_2 + \sin x_1 \cos x_2 \\ -(\sin x_1 \cos x_2 + \cos x_1 \sin x_2) & \cos x_1 \cos x_2 - \sin x_1 \sin x_2 \end{bmatrix} \\
&= \begin{bmatrix} \cos(x_1 + x_2) & -\sin(x_1 + x_2) \\ \sin(x_1 + x_2) & \cos(x_1 + x_2) \end{bmatrix} \\
&= \phi(x_1 + x + 2)
\end{aligned}$$

Thus ϕ is a homomorphism.

Also,

$$\det(\phi(x)) = \det \begin{bmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{bmatrix} = \cos^2 x + \sin^2 x = 1,$$

so $\phi(x) \in \mathbf{SL}_2(\mathbb{R})$. With $a = \cos x$ and $b = \sin x$, it follows that $\phi(x) \in M$ for every $x \in \mathbb{R}$. To show that ϕ is onto M, let $A = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ be an arbitrary member of M. Since $\det(A) = a^2 + b^2 = 1$, so that $a^2 = 1 - b^2$. Since b^2 is nonnegative, we have $a^2 \in [0, 1]$, so $a \in [-1, 1]$.

Let $x = \arccos a$, so that $a = \cos x$. Then $b = \sqrt{1 - \cos^2 x} = \pm \sin x$. If $b = \sin x$, then $\phi(x) = A$. If $b = -\sin x$, then (since sin is an odd function), $\phi(-x) = A$. Thus ϕ is onto M, and $\phi(\mathbb{R}) = M$.

Since M is the image of a homomorphism, M is a group, and $M \leq \mathbf{SL}_2(\mathbb{R})$. The identity in M is the identity matrix, and we see that $\ker(\phi) = 2\pi\mathbb{Z}$. By the isomorphism theorem, $M \cong \mathbb{R}/2\pi\mathbb{Z}$. $\square$

Problem 5. Let $X \subset \mathbb{R}^2$ be a subset of the cartesian plane. If $\vec{v}, \vec{w} \in X$, the distance between $\vec{v}$ and $\vec{w}$ is denoted $d(\vec{v}, \vec{w})$. An *isometry* of X is a function $f : X \to X$ which preserves the distance between any to points, so that

$$d(\vec{v}, \vec{w}) = d(f(\vec{v}), f(\vec{w})).$$

Let

$$\mathrm{Iso}(X) = \{f : X \to X \mid f \text{ is an isometry}\}.$$

This is a group under composition.

For example, if X is a square, the isometries of X are rotations and reflections, and $\mathrm{Iso}(X) \cong D_4$; that is, the group of isometries of X is isomorphic to the dihedral group on 4 points.

Describe $\mathrm{Iso}(X)$ (number of elements, elements and their orders, how elements interact, interesting subgroups, etc.) in each of these cases

(a) $X = \{(x, y) \in \mathbb{R}^2 \mid y = x^2\}$ (a parabola)

(b) $X = \{(x, y) \in \mathbb{R}^2 \mid \frac{x^2}{9} + \frac{y^2}{4} = 1\}$ (an ellipse)

(c) $X = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ (a circle)

(d) $X = \{(x, y) \in \mathbb{R}^2 \mid y = \tan(x)\}$

Solution.

(a) In this case, $\mathrm{Iso}(X) \cong C_2$ (cyclic of order two); it contains the identity and a reflection.

(b) In this case, $\mathrm{Iso}(X) \cong K_4$; it contains two reflections, one rotation of order two, and the identity. Note that $\mathrm{Iso}(X)$ is not isomorphic to D_4; the ninety degree rotations and the reflections through the sides of the square do not have analogous isometries of X.

(c) In this case, $\mathrm{Iso}(X) \cong \mathbb{U} \cong M$ from the previous problem.

(d) In this case, $\mathrm{Iso}(X)$ consists of horizontal translations by multiples of π, and rotations by 180° about any of the x-intercepts.

Let $\alpha_k : \mathbb{R}^2 \to \mathbb{R}^2$ be given by $\alpha_k(x, y) = (x + \pi k, y)$. Then $\alpha_k \in \mathrm{Iso}(X)$ is a horizontal translation. Note that α_k is an element of infinite order, and $\alpha_k^{-1} = \alpha_{-k}$.

Let $\beta_j : \mathbb{R}^2 \to \mathbb{R}^2$ be given by $\beta_j(x, y) = (\pi j - x, -y)$. Then $\beta_j \in \mathrm{Iso}(X)$ is rotation around the point $(\pi j, 0)$. Note that β_j is an element of order two, so that $\beta_j^{-1} = \beta_j$.

Let $A = \{\alpha_k \in \mathrm{Iso}(X) \mid k \in \mathbb{Z}\}$; this is the set of horizontal translations. Clearly, $T \leq \mathrm{Iso}(X)$, and $T \cong \mathbb{Z}$. Moreover, T is normal in $\mathrm{Iso}(X)$; in fact,

$$\begin{aligned}
\beta_j^{-1}\alpha_k\beta_j(x, y) & \\
&= \beta_j\alpha_k\beta_j(x, y) \\
&= \beta_j\alpha_k(\pi j - x, -y) \\
&= \beta_j((\pi j - x) + \pi k, -y) \\
&= \beta_j(\pi(k + j) - x, -y) \\
&= (\pi j - (\pi(k + j) - x), y) \\
&= (x - \pi k, y) \\
&= \alpha_{-k}(x, y).
\end{aligned}$$

That is, conjugation of α_k by β_j inverts α_k; in particular, $T \triangleleft \mathrm{Iso}(X)$. Clearly, $\mathrm{Iso}(X)/T \cong C_2 \cong \langle\beta_0\rangle$. ☐