HW2, due Wednesday, February 15
Math 403, Spring 2017
Patrick Brosnan, Instructor

Practice Problems: Do the following problems from Herstein for practice, but do not turn them in. The format below is that **H4.5** means "Chapter 4, Section 5 of Herstein."

H1.5: 1, 5, 7, 13, 14
H1.6: 2
H1.4: 4, 17
H2.1: 1, 8, 21, 28, 29

Reminders from Class

In class, I plan to talk about binary operations (magmas) and associative binary operations (monoids) before introducing the concept of a group. This is not in Herstein's book. So, depending on how good your notes are when you start this problem set, these reminders from class may be useful.

Recall from class that a *magma* is a set M with a binary operation $* : M \times M \to M$ usually written as $(x,y) \mapsto x*y$ or just $(x,y) = xy$ if $*$ is understood. A magma is *commutative* if $xy = yx$ for all x,y in M and *associative* if $(xy)z = x(yz)$ for all x,y,z in M. An identity element in a magma M is an element e such that $xe = ex = x$ for all $x \in M$. If an identity element exists in a magma, it is unique.

An associative magma M with identity element e is called a *monoid*. An element x in a monoid is said to be *invertible* if there exists $y \in M$ such that $xy = yx = e$. In this case, y is unique and is called the inverse of x. Usually we write it as $y = x^{-1}$. (If the binary operation is written as "+" then we write $-x$ instead of x^{-1}. We only write the binary operation as "+" for commutative monoids.) A group is a monoid G in which every element is invertible.

A subset H of a magma M is called a *submagma* if it is closed under the binary operation of M. That is, it is a submagma if $xy \in H$ for all $x,y \in H$. A subset H of a monoid M is a *submonoid*, if H is a submagma containing the identity element of M. If M is a monoid then the subset $M^\times$ of M consisting of all invertible elements of M is a submonoid. Clearly $M^\times$ is also a group under the binary operation inherited from M.

A *subgroup* of a group G is a submonoid H which is also a group. A subset H of G is a subgroup if and only if H is non-empty and $x,y \in H \Rightarrow xy^{-1} \in H$.

Commutative groups are also called *abelian* groups. This is in honor of the mathematician Niels Henrik Abel.

Graded Problems: Work the following problems for a grade.

1 (20 points)**.** Compute $d = (201,57)$ and find integers x and y such that $201x + 57y = d$.

2 (15 points)**.** Let $2 = p_1$, $3 = p_2$, $5 = p_3$, etc. In other words, for each positive integer k, let p_k denote the k-th smallest prime. Find the smallest $k > 1$ such that $p_1 p_2 \cdots p_k - 1$ is not a prime.

(**Bonus 5 point**) Find the smallest k such that $p_1 p_2 \cdots p_k + 1$ is not prime.

3 (15 points)**.** Write $M_2(\mathbb{R})$ for the set of 2×2 matrices

$$X = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with a,b,c and d real.

(1) Show that $M_2(\mathbb{R})$ is a monoid with the operation of matrix multiplication. Make sure to say what the identity element is.
(2) Show that the set $\mathbf{GL}_2(\mathbb{R})$ of invertible elements in $M_2(\mathbb{R})$ consists of the the matrices X as above for which $ad-bc\neq 0$.
(3) Conclude that $\mathbf{GL}_2(\mathbb{R})$ is a group. What is the inverse of the matrix X above (assuming $ad-bc\neq 0$)?

4 (40 points)**.** Write $C := \{(x,y)\in\mathbb{R}^2 : x^2+y^2=1\}$ for the unit circle in $\mathbb{R}^2$, and write $\mathbf{O}(2) := \{X\in\mathbf{GL}_2(\mathbb{R}) : X(C)=C\}$.

(1) Show the matrix
$$T := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
is in $\mathbf{O}(2)$.
(2) Show that, for any $\theta\in\mathbb{R}$, the matrices
$$R(\theta) := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$
and $TR(\theta)$ are in $\mathbf{O}(2)$.
(3) Suppose $X\in\mathbf{O}(2)$. Show that either $X=R(\theta)$ or $X=TR(\theta)$ for some θ. One way to do this is to set $\mathbf{e}=(1,0)$, $\mathbf{f}=(0,1)$ and $\mathbf{w}=(\sqrt{2}/2,\sqrt{2}/2)$. Then use the fact that $X\mathbf{e}, X\mathbf{f}$ and $X\mathbf{w}$ all lie on the unit circle.
(4) Show that $R(\theta)^{-1}=R(-\theta)$ while $T^{-1}=T$.
(5) Show that $TR(\theta)T=R(-\theta)$.
(6) Show that $\mathbf{O}(2)$ is a subgroup of $\mathbf{GL}_2(\mathbb{R})$.
(7) Show that $\mathbf{O}(2)$ is not abelian.
(8) Let S denote the subset of $\mathbf{O}(2)$ consisting of matrices of the form $R(\theta)$ for some $\theta\in\mathbb{R}$. Show that $R(\theta)R(\tau)=R(\theta+\tau)$ and, using this, conclude that S a subgroup of $\mathbf{O}(2)$ which is abelian.

5 (10 points)**.** Let $S_2(\mathbb{R})$ denote the set of symmetric 2×2 matrices. That is $S_2(\mathbb{R})$ is the set of matrices of the form

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix}$$

with a,b,c in $\mathbb{R}$.

(1) Show that $S_2(\mathbb{R})$ is closed under the operation $X*Y=(XY+YX)/2$. Here XY and YX denote usual matrix multiplication.
(2) Show that the binary operation $*$ is commuatitive but not associative.