Math 4400 Homework 5
Due: Friday, June 23rd, 2017

Feel free to work with your classmates, but everyone must turn in their own assignment. Please make a note of who you worked with on each problem. Let me know if you find a typo, or you're stuck on any of the problems.

1. (5 points) Prove that multiplication of 2×2 matrices with real entries is associative.

> **Solution:** This is just a simple, but tedious computation: we let L, M, N be three arbitrary 2×2 matrices with real entries. Then there exist real numbers $a, b, c, d, e, f, g, h, i, j, k, l \in \mathbb{R}$ such that
>
> $$L = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad M = \begin{pmatrix} e & f \\ g & h \end{pmatrix}, \quad N = \begin{pmatrix} i & j \\ k & l \end{pmatrix}$$
>
> Then
>
> $$L \cdot M = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}$$
>
> which means
>
> $$(L \cdot M) \cdot N = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix} \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix} = \begin{pmatrix} (ae + bg)i + (af + bh)k & (ae + bg)j + (af + bh)l \\ (cd + dg)i + (cf + dh)k & (ce + dg)j + (cf + dh)l \end{pmatrix}$$
>
> Further,
>
> $$M \cdot N = \begin{pmatrix} ei + fk & ej + fl \\ gi + hk & gj + hl \end{pmatrix}$$
>
> which means
>
> $$L \cdot (M \cdot N) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} ei + fk & ej + fl \\ gi + hk & gj + hl \end{pmatrix} = \begin{pmatrix} a(ei + fk) + b(gi + hk) & a(ej + fl) + b(gj + hl) \\ c(ei + fk) + d(gi + hk) & c(ej + fl) + d(gj + hl) \end{pmatrix}$$
>
> We wish to show that $(L \cdot M) \cdot N = L \cdot (M \cdot N)$. So we just have to check the following equalities:
>
> $$\begin{aligned} (ae + bg)i + (af + bh)k &= a(ei + fk) + b(gi + hk) \\ (ae + bg)j + (af + bh)l &= a(ej + fl) + b(gj + hl) \\ (cd + dg)i + (cf + dh)k &= c(ei + fk) + d(gi + hk) \\ (ce + dg)j + (cf + dh)l &= c(ej + fl) + d(gj + hl) \end{aligned}$$
>
> which just follows from the associativity, distributivity, and commutativity properties of the real numbers.

2. (a) (5 points) Let $GL_2(\mathbb{R})$ be the set of invertible 2×2 matrices with real entries. Prove that $GL_2(\mathbb{R})$ is a group under multiplication

> **Solution:** Let $A, B \in GL_2(\mathbb{R})$. Then, by definition A has an inverse matrix A^{-1} and B has an invnerse matrix B^{-1}. We note that
>
> $$(AB)(B^{-1}A^{-1}) = (B^{-1}A^{-1})AB = I$$
>
> Where I is the identity matrix. Thus AB is also an invertible 2×2 matrix with real entries. This shows multiplication is a binary operation on $GL_2(\mathbb{R})$.

Next, we have to check that $GL_2(\mathbb{R})$ has an identity element. Since I is invertible, we see that $I \in GL_2(\mathbb{R})$. Since

$$IM = MI = M$$

for *all* 2×2 matrices, we see that I is the identity element of $GL_2(\mathbb{R})$.

By problem 1, multiplication is an associative operation

Finally we check that each element of $GL_2(\mathbb{R})$ has an inverse in $GL_2(\mathbb{R})$. In other words, we have to check that, whenever A is an invertible 2×2 matrix with real entries, its inverse matrix A^{-1} is also an invertible 2×2 matrix with real entries. But this is clear: the inverse of A^{-1} is A.

(b) (5 points) Let $SL_2(\mathbb{Z})$ be the set of 2×2 matrices with integer entries and determinant 1. Prove that $SL_2(\mathbb{Z})$ is a subgroup of $GL_2(\mathbb{R})$. This closely related to the so-called “modular group”, which is one of the most interesting and important groups in number theory.

Solution: Let $M, N \in SL_2(\mathbb{Z})$ be arbitrary. By a proposition we showed in class (on 6/12/17), it suffices to check that $MN^{-1} \in SL_2(\mathbb{Z})$. To see this, we recall the formula for the inverse of a 2×2 matrix: we can write N as

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

for some integers $a, b, c, d \in \mathbb{Z}$. Then the inverse of N is given by

$$N^{-1} = \frac{1}{\det N} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

(Since $N \in SL_2(\mathbb{Z})$, we know that $\det N = 1$). Thus N^{-1} is also a 2×2 matrix with integer entries. Further, since

$$NN^{-1} = I,$$

we have

$$\det(NN^{-1}) = \det I = 1$$

Since $\det(AB) = \det(A)\det(B)$ for any pair of matrices A and B, we see

$$\det(N^{-1}) = 1/\det(N) = 1,$$

again using the fact that $\det N = 1$ be the definition of $SL_2(\mathbb{Z})$.

It's clear from the definition of matrix multiplication that the product of two matrices with integer entries also has integer entries. Thus MN^{-1} has integer entries. Further, $\det(MN^{-1}) = \det(M)\det(N^{-1}) = 1 \cdot 1 = 1$. Thus $MN^{-1} \in SL_2(\mathbb{Z})$, as desired.

(c) (5 points) Let $S = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| \, a, b, c \in \mathbb{R}, ac \neq 0 \right\}$. Prove that S is a subgroup of $GL_2(\mathbb{R})$.

Solution: Using the formula for the inverse of 2×2 matrix, we compute:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} d & e \\ 0 & f \end{pmatrix}^{-1} = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{d} & -e/df \\ 0 & \frac{1}{f} \end{pmatrix} = \begin{pmatrix} \frac{a}{d} & \frac{-ea}{df} + \frac{b}{f} \\ 0 & \frac{c}{f} \end{pmatrix} \in S$$

By the characterization of subgroups that we discussed in class, this shows S is a subgroup of $GL_2(\mathbb{R})$. Note that $d \neq 0$ and $f \neq 0$, since $df \neq 0$, so we're allowed to divide by d and f above.

(d) (5 points) Let $T = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| \; a \in \mathbb{R} \right\}$. Prove that T is a subgroup of S.

Solution: Same as above, we compute:

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a-b \\ 0 & 1 \end{pmatrix} \in T$$

Note that T is actually abelian:

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$$

This group is usually denoted $U_2(\mathbb{R})$, and its elements are called *unipotent* matrices.

3. (a) (2 points) Let G be a group. Prove that if $a, x, y \in G$ and $ax = ay$, then $x = y$.

Solution: By definition of a group, a has an inverse $a^{-1} \in G$. Thus $a^{-1}(ax) = a^{-1}(ay)$. By the associativity property, we see that $(a^{-1}a)x = (a^{-1}a)y$. By definition of inverses, $a^{-1}a = e$, so we have $ex = ey$. Thus $x = y$.

(b) (2 points) Prove that the identity element of a group is unique. In other words, if G is a group, and $e, e' \in G$ are elements such that $eg = ge = g$ and $e'g = ge' = g$ for all $g \in G$, then $e = e'$.

Solution: $ee' = e$, since e' is an identity element of G. Also, $ee' = e'$, since e is an identity element of G. Thus $e = ee' = e'$.

(c) (2 points) Prove that the inverse of a group element is unique. In other words, if G is a group, and $g, h, h' \in G$ are elements such that

$$gh = hg = e$$
$$gh' = h'g = e$$

then $h = h'$.

Solution: We have $h(gh') = he = h$. But also $h(gh') = (hg)h' = eh' = h'$. Thus $h = hgh' = h'$.

4. Are the following groups? If yes, prove it. If not, say why not

(a) (2 points) $\mathbb{Z}$ with the binary operation $\star$ defined by $a \star b = 2a + b$

Solution: This is not a group since $\star$ is not associative:

$$(a \star b) \star c = 2(2a + b) + c = 4a + 2b + c$$

whereas

$$a \star (b \star c) = 2a + 2b + c$$

and these are not the same as long as $a \neq 0$.

(b) (2 points) $\mathbb{N}$ under multiplication

Solution: This is not a group since not every element of $\mathbb{N}$ has an inverse element in $\mathbb{N}$. For instance, the multaplicative inverse of 2 is $\frac{1}{2}$, but $\frac{1}{2} \notin \mathbb{N}$.

(c) (2 points) The set $\{1, -1\}$ under multiplication.

Solution: This is a group: multiplication is indeed a binary operation on the set, 1 is the identity element, multiplication is associative, and each element is its own inverse.

(d) (2 points) $\mathbb{Z}/15\mathbb{Z}$ under addition

Solution: This is a group: if $[a]_{15}$ and $[b]_{15}$ are elements of $\mathbb{Z}/15\mathbb{Z}$, then $[a] + [b] = [a + b] \in \mathbb{Z}/15\mathbb{Z}$, so addition is indeed a binary operation. The identity element is $[0]$ since, by definition of addition of equivalence classes, $[0] + [a] = [0 + a] = [a]$ for all $[a] \in \mathbb{Z}/15\mathbb{Z}$, and similarly $[a] + [0] = [a]$. Addition of equivalence classes is associative:

$$([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c] = [a + (b + c)] = [a] + [b + c] = [a] + ([b] + [c])$$

Finally, the inverse of any element $[a] \in \mathbb{Z}/15\mathbb{Z}$ is $[-a]$ as $[a] + [-a] = [-a] + [a] = [0]$.

(e) (2 points) $\mathbb{Z}/15\mathbb{Z}$ under multiplication

Solution: This is not a group, as not every element has a multaplicative inverse modulo 15. For instance, $[0]$ can't have a mulaplicative inverse, since $[0] \cdot [a] = [0]$ for all $[a] \in \mathbb{Z}/15\mathbb{Z}$.

(f) (2 points) $M_{2\times 2}(\mathbb{R})$, with the binary operation $\star$, defined by $A \star B = AB - BA$.

Solution: This isn't a group for many reasons. One is that there's no identity element (thanks to James for pointing this out): if $A \star E = E \star A = A$, for some $A, E \in M_{2\times 2}(\mathbb{R})$, then $AE - EA = EA - AE$, so $2AE = 2EA$ and $EA = AE$. But that means $A \star E = AE - EA = 0$. So if $A \neq 0$, then $A \star E \neq E \star A$ for any E.

This operation turns out not be associative either; it satisfies the so-called *Jacobi identity*:

$$(A \star B) \star C - A \star (B \star C) = B \star (C \star A)$$

for all matrices A, B, C.

5. (5 points) Let $(G, \cdot)$ and $(H, *)$ be two groups. Show that $G \times H$ is a group, under the binary operation $\star$ defined by

$$(g, h) \star (g', h') = (g \cdot g', h * h')$$

Solution: Let (g, h) and (g', h') be two elements of $G \times H$. Then $g \cdot g' \in G$ and $h \times h' \in H$ since, by defintion, $\cdot$ is a binary operation on G and $*$ is a binary operation on H. Thus $(g, h) \star (g', h') = (g \cdot g', h * h') \in G \times H$, so $\star$ is indeed a binary operation.

By definition of a group, G has some identity element e_G and H has some identity element e_H. Then (e_G, e_H) is the identity element of $G \times H$: indeed, for all $(g, h) \in G \times H$, we have:

$$(g, h) \star (e_G, e_H) = (g \cdot e_g, h * e_H) = (g, h),$$
$$(e_G, e_H) \star (g, h) = (e_g \cdot g, e_H * h) = (g, h)$$

Also, we know that g has some inverse $g^{-1} \in G$ and h has some inverse $h^{-1} inH$. Thus, $(g^{-1}, h^{-1}) \in G \times H$. We check:

$$(g,h) \star (g^{-1}, h^{-1}) = (g \cdot g^{-1}, h * h^{-1}) = (e_G, e_H)$$
$$(g^{-1}, h^{-1}) \star (g,h) = (g^{-1} \cdot g, h^{-1} * h) = (e_G, e_H)$$

Thus, $(g,h)^{-1} = (g^{-1}, h^{-1}) \in G \times H$, so every element of $G \times H$ has an inverse.
Finally, let $(g,h), (g', h'), (g'', h'') \in G \times H$. Then:

$$\begin{aligned}
(g,h) \star ((g',h') \star (g'',h'')) &= (g,h) \star (g' \cdot g'', h' * h'') \\
&= (g \cdot (g' \cdot g''), h * (h' * h'')) \\
&= ((g \cdot g') \cdot g'', (h * h') * h'') \text{ because } \cdot \text{ and } * \text{ are associative} \\
&= (g \cdot g', h * h') \star (g'', h'') \\
&= ((g,h) \star (g',h')) \star (g'', h'')
\end{aligned}$$

So $\star$ is an associative binary operation on $G \times H$.

6. (5 points) Prove that cyclic groups are abelian

Solution: Let G be a cyclic group. That means there exists some element $g \in G$ such that $G = \langle g \rangle$. Let $x, y \in G$ be arbitrary elements of G. Since $G = \langle g \rangle$, that means $x, y \in \langle g \rangle$. By definition, that means there exist some integers i, j such that $x = g^i$ and $y = g^j$. But this means that

$$x \cdot y = g^i \cdot g^j = g^{i+j} = g^j \cdot g^i = y \cdot x$$

just using the exponent rules. This shows that G is abelian.

7. (a) (10 points) Let $a, b \in \mathbb{N}$. Show that $\operatorname{lcm}(a,b) = \dfrac{ab}{\gcd(a,b)}$.

Solution: This is easier if we use prime factorizations: let $p_1, \ldots, p_n$ be all the distinct primes appearing in the factorizations of a and b. Then there exist natural numbers $e_i, f_i \in \mathbb{N}$ such that

$$a = p_1^{e_1} \cdots p_n^{e_n}$$

and

$$b = p_1^{f_1} \cdot p_n^{f_n}$$

Then

$$\operatorname{lcm}(a,b) \cdot \gcd(a,b) = p_1^{\min(e_1,f_1)+\max(e_1,f_1)} \cdots p_n^{\min(e_n,f_n)+\max(e_n,f_n)}$$

Note that $\min(e_i, f_i) + \max(e_i, f_i) = e_i + f_i$ for all i. Thus,

$$\operatorname{lcm}(a,b) \cdot \gcd(a,b) = p_1^{e_1+f_1} \cdots p_n^{e_n+f_n} = ab,$$

as desired.
There's also way to prove this using Bezout's lemma, but I have a thesis to write ⌣̈

(b) (5 points) Let $a, n \in \mathbb{N}$ with $n \neq 0$. Prove that $o([a]) = \dfrac{n}{\gcd(a,n)}$ in $\mathbb{Z}/n\mathbb{Z}$

Solution: Note that $n[a] = [0]$, so $o([a]) < \infty$. Thus, there exists some integer $k > 0$ such that $o([a]) = k$.
Since $k[a] = [0]$, that means $n \mid ka$. In other words, ka is a common multiple of n and a. On the other hand, if $c > 0$ is another common multiple of a and n, then $\frac{c}{a}[a] = [c] = [0]$ in $\mathbb{Z}/n\mathbb{Z}$. By the definition of $o([a])$, we must have $k \leq \frac{c}{a}$, and thus $ka \leq \frac{c}{a}a = c$. So we've just shown that ka is the least common multiple of a and n. By part (a) above, we see that $ka = \frac{an}{\gcd(a,n)}$, so $k = \frac{n}{\gcd(a,n)}$, as desired.

8. (5 points) Can a non-abelian group have an abelian subgroup? If yes, give an example. If not, prove why not.

Solution: Yes: for instance, in problem 2, we saw that T is a subgroup of $GL_2(\mathbb{R})$. T is abelian but $GL_2(\mathbb{R})$ is not.

9. (5 points) Let p be a prime number and let G be a group of order p. Prove that G is abelian.

Solution: Since $\#G = p > 1$, G has an element that's not the identity element, e. Let $g \in G$ such an element. By Lagrange's theorem, we know that $o(g) \mid \#G$, which means $o(g) = 1$ or $o(g) = p$. Note that if $o(g) = 1$, that means, by definition, that $g^1 = e$. But g^1 is just g. Since $g \neq e$, we must have $o(g) = p$. We also saw in class that $o(g) = \#\langle g \rangle$, so $\#\langle g \rangle = p$. Since $\langle g \rangle \subseteq G$ and both of these sets of the same size, we see that $\langle g \rangle = G$. In other words, G is cyclic. By problem 6, cyclic groups are always abelian, so G must be abelian.

10. (10 points) Let G be a group of order 4. Show that G is abelian. (Hint: we can write $G = \{e, a, b, c\}$ where e, a, b, c are all distinct. What can $o(a)$ be? Break the problem up into cases) It turns out there are only two different groups of order 4: $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Solution: Let G be a group of order 4. If G is cyclic, then G must be abelian by problem 6. So suppose G is not cyclic. Then no element of G has order 4. By Lagrange's theorem, each element must then have order 1 or 2. Thus, for all $a \in G$, we have $a^2 = e$. Now let a, b be arbitrary. Then $(ab)^2 = abab = e$. Multiplying by a on the left and by b on the right, we get $a^2bab^2 = ab$. But $a^2 = b^2 = e$, so this means $ba = ab$, as desired.