Math 30810 Honors Algebra 3
Homework 2

Andrei Jorza

Due Thursday, September 8

Do any 8 of the following 10 questions. Artin a.b.c means chapter a, section b, exercise c.

1. Artin 2.1.1 on page 69.

   Proof. We check $(ab)c = ac = a$ and $a(bc) = ab = a$ so the composition law is associative.

   If e is an identity then $ea = a$ for all $a \in S$ but the composition law dictates that $ea = e$. Therefore if S has an identity then $S = \{e\}$. $\square$

2. Artin 2.2.2 on page 69.

   Proof. Write S for the set with composition law and identity and $G = \{x \in S \mid x \text{ has an inverse}\}$. Clearly $e \in G$ as $e^{-1} = e$. Also, if $x, y \in G$ then $(xy)^{-1} = y^{-1}x^{-1}$ so xy also has an inverse and therefore $xy \in G$. Finally, $(x^{-1})^{-1} = x$ so x^{-1} also has an inverse and therefore $x^{-1} \in G$. This implies that G is a group. $\square$

3. Artin 2.2.4 on page 70.

   Proof. (a): Yes. If you invert or multiply matrices with real coefficients you still get a matrix with real coefficients.

   (b): Yes.

   (c): No as -1 is not a positive integer.

   (d): Yes. If you multiply or divide positive reals you still get positive reals.

   (e): No. H is not even a subset of G. $\square$

4. Artin 2.2.6 on page 70.

   Proof. First, we check associativity. But $(a * b) * c = c(ba) = (cb)a = (b * c)a = a * (b * c)$ from the associativity of multiplication in G. Next, if e is an identity in G then $x * e = ex = x$ and $e * x = xe = x$ so e is an identity in G°. Finally, if x has inverse y in G then $x * y = yx = e$ and $y * x = xy = e$ so y is also an inverse in G°. $\square$

5. Let B be the subset of $\mathrm{GL}_n(\mathbb{R})$ consisting of upper-triangular matrices. Show that B is a subgroup of $\mathrm{GL}_n(\mathbb{R})$.

Proof. First, $I_n \in B$.

Next, let $A = (a_{ij})$ and $B = (b_{ij})$ be upper triangular with $a_{ij} = b_{ij} = 0$ for $i > j$. Write $AB = C = (c_{ij})$. For $i > j$

$$c_{ij} = \sum_k a_{ik} b_{kj} = \sum_{k<i} 0 \cdot b_{kj} + \sum_{k \geq i} a_{ij} \cdot 0 = 0$$

as when $k < i$ we have $a_{ik} = 0$ and if $k \geq i > j$ then $k > j$ and so $b_{kj} = 0$. This means that AB is also upper triangular.

Finally, we need that if A is upper triangular in $\mathrm{GL}_n(\mathbb{R})$ then A^{-1} is also upper triangular. There's a few ways to do this, here are four:

Method A. I learned this from Amelia's solution. I think it's the easiest. Recall that the cofactor matrix $A^* = (b_{ij})$ satisfies $AA^* = \det(A) I_n$ where $b_{ij} = (-1)^{i+j} \det A_{ji}$ with A_{ij} is the minor where you remove the i-th row and j-column. Then $A^{-1} = (\det A)^{-1} A^*$ so it's enough to show that A^* is upper triangular. Suppose $i > j$. We'd like to show that $b_{ij} = 0$ which is equivalent to $\det A_{ji} = 0$. But A_{ji} will be, simply by inspection, upper triangular with 0s on the diagonal in positions (j, j), $(j + 1, j + 1)$, ..., $(i - 1, i - 1)$ and so $\det A_{ji} = 0$.

Method B (Uses homework 1) I learned this one from Patrick's solution. Suppose your matrix is $A = (a_{ij})$ upper triangular invertible with nonzero entries on the diagonal. The diagonal matrix $B = \mathrm{diag}(a_{11}, \ldots, a_{nn})$ has inverse $B^{-1} = \mathrm{diag}(a_{11}^{-1}, \ldots, a_{nn}^{-1})$ and if you look at AB^{-1} you'll see that it is upper triangular with 1-s on the diagonal. Write $N = AB^{-1} - I_n$ which will be upper triangular with 0s on the diagonal. Then N^2 will have 0s on the diagonals $j = i$ and $j = i + 1$ and you can check that N^k will have 0s on the diagonals $0 \leq j - i \leq k - 1$. When $k = n + 1$ this implies that N is nilpotent. But you already know that if N is nilpotent then $I_n + N$ is invertible from the first homework, with inverse $I_n - N + N^2 - \cdots$ which will then be upper triangular. Therefore $A = (I_n + N)B$ is also invertible with inverse $B^{-1}(I_n + N)^{-1}$ which is then also upper triangular.

Method C (Induction). This is the method that will yield most positive results in general. Please read this. We'll show by induction on n that A^{-1} is upper triangular. The base case of the induction is $n = 1$ in which case $A = (a_{11})$ and its inverse is (a_{11}^{-1}).

For the inductive step, let $A_{11} = (a_{ij})_{i,j>1}$. Since A_{11} is upper triangular with $n-1$ rows and columns the inductive hypothesis implies that A_{11}^{-1} is upper triangular. The simply compute

$$A^{-1} = \begin{pmatrix} a_{11} & \vec{a} \\ 0_{n-1,1} & A_{11} \end{pmatrix}^{-1} = \begin{pmatrix} a_{11}^{-1} & -a_{11}^{-1} \vec{a} A_{11}^{-1} \\ 0_{n-1,1} & A_{11}^{-1} \end{pmatrix}$$

which is upper triangular as A_{11}^{-1} is upper triangular.

Method D (Brute force) This is somewhat nasty, you can skip it. I only included it to show it's possible. We seek $B = (b_{ij})$ such that $AB = I_n$, i.e., $\sum a_{ik} b_{kj} = \delta_{ij}$ where $I_n = (\delta_{ij})$ so δ_{ij} is 1 if $i = j$ and 0 if $i \neq j$. As A is upper triangular this can be rewritten as $\sum_{k \geq i} a_{ik} b_{kj} = \delta_{ij}$. Let's write these equations in more detail. For $i = n$ get $a_{nn} b_{nj} = \delta_{nj}$ which immediately yields $b_{nj} = a_{nn}^{-1} \delta_{nj}$ for $j \leq n$. Note that among these b_{nn} is nonzero and the other b_{nj} are 0. (Since A is invertible remember that all the diagonal terms a_{ii} are invertible.)

Next, for $i = n - 1$ get $a_{n-1,n-1} b_{n-1,j} + a_{n-1,n} b_{n,j} = \delta_{n-1,j}$. We already know $b_{n,j}$ for all j and so we compute

$$b_{n-1,j} = a_{n-1,n-1}^{-1} (\delta_{n-1,j} - a_{n-1,n} b_{n,j})$$

noting that if $j < n - 1$ then $\delta_{n-1,j} = 0$ and $b_{n,j} = 0$ and so $b_{n-1,j} = 0$.

Keep going like this and see that you can determine all $b_{i,j}$ and that the inverse matrix $B = (b_{ij})$ is upper triangular.

Method E (Cool calculus method) This is a nice calculusy method that has lots of uses in general.

Remember that the Taylor series $e^x = 1 + x + x^2/2! + x^3/3! + \cdots$ converges everywhere and that the Taylor series $\log(1+x) = x - x^2/2 + x^3/3 - \cdots$ converges where $|x| < 1$. We can plug in matrices instead of the real variable x and we can make sense of $e^A = 1 + A + A^2/2! + A^3/3! + \cdots$ for every matrix A. If A happens to be upper triangular then so is every power A^k and so e^A is also upper triangular.

What about $\log(1+A)$? If A is upper triangular with 0-s on the diagonal then A^2 has 0-s on the diagonal $i = j$ AND on the diagonal $j = i+1$, A^3 has zeros on the diagonals $0 \leq j - i \leq 2$ and so on all the way to $A^n = 0$, where A is $n \times n$. This means that the Taylor series $\log(1+A) = A - A^2/2 + \cdots$ terminates at $(-1)^{n-1}A^n/n$ so this power series is a well defined finite sum with no issues of convergence. Again, since every A^k is upper triangular, so is $\log(1+A)$.

Let's get back to our problem at hand, namely: if A is upper triangular invertible then A^{-1} is also upper triangular. Look at the diagonal matrix $B = \operatorname{diag}(a_{11}, \ldots, a_{nn})$ which has inverse $B^{-1} = \operatorname{diag}(a_{11}^{-1}, \ldots, a_{nn}^{-1})$ (it's invertible as $\det(A) = \prod a_{ii} \neq 0$). Then AB^{-1} has 1-s on the diagonal and so $X = AB^{-1} - 1$ has 0-s on the diagonal which means that $C = \log(AB^{-1}) = \log(1+X)$ makes sense. Moreover, since X is upper triangular, so is C. Now

$$e^{-C} = e^{-\log(AB^{-1})} = (e^{\log(AB^{-1})})^{-1} = (AB^{-1})^{-1} = BA^{-1}$$

so $A^{-1} = B^{-1}e^{-C}$. We're now done because C is upper triangular, therefore so is e^{-C} and therefore so is $A^{-1} = B^{-1}e^{-C}$.

Remark: This entire proof was based on the idea that $\log(x^{-1}) = -\log(x)$ so after log inversion is very simple. We only needed to make sense of all these operations for matrices. While this seems over the top, this method is extremely useful and often used in differential equations, so don't disregard it.

□

6. Let T be the subset of $\mathrm{GL}_n(\mathbb{R})$ consisting of diagonal matrices. Show that T is a subgroup of $\mathrm{GL}_n(\mathbb{R})$.

Proof. Note that $\operatorname{diag}(x_1, \ldots, x_n)\operatorname{diag}(y_1, \ldots, y_n) = \operatorname{diag}(x_1y_1, \ldots, x_ny_n)$ and $\operatorname{diag}(x_1, \ldots, x_n)^{-1} = \operatorname{diag}(x_1^{-1}, \ldots, x_n^{-1})$. □

7. Show that the set of matrices

$$H = \left\{ \begin{pmatrix} 1 & x_1 & x_2 & \ldots & x_{n-1} & x_n & z \\ 0 & 1 & 0 & 0 & \ldots & 0 & y_1 \\ 0 & 0 & 1 & 0 & \ldots & 0 & y_2 \\ & & & \ddots & & & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 1 & y_n \\ 0 & 0 & 0 & \ldots & 0 & 0 & 1 \end{pmatrix} \mid x_1, \ldots, x_n, y_1, \ldots, y_n, z \in \mathbb{R} \right\}$$

forms a subgroup of $\mathrm{GL}_{n+2}(\mathbb{R})$. It is called the Heisenberg group.

Proof. Write $m(\vec{x}, \vec{y}, z)$ for the matrix in the statement. Clearly $m(\vec{0}, \vec{0}, 0) = I_n$ is an identity. Also,

$$m(\vec{x}, \vec{y}, z)m(\vec{x'}, \vec{y'}, z') = m(\vec{x} + \vec{x'}, \vec{y} + \vec{y'}, z + z' + x_1y_1' + \cdots + x_ny_n')$$

so H is closed under multiplication.

Finally,

$$m(\vec{x}, \vec{y}, z)^{-1} = m(-\vec{x}, -\vec{y}, -z + x_1y_1 + \cdots + x_ny_n)$$

□

8. For a matrix $A \in M_{n\times n}(\mathbb{R})$, let A^t be the transpose matrix, so that the ij-entry of A^t is the ji entry of A. Prove that if $A \in \mathrm{GL}_n(\mathbb{R})$, then $(A^{-1})^t = (A^t)^{-1}$. [Hint: recall that for matrices A and B in $M_{n\times n}(\mathbb{R})$, $(AB)^t = B^tA^t$.]

   Proof. It's enough to check that $(A^{-1})^tA^t = I_n$. But $(A^{-1})^tA^t = (A\cdot A^{-1})^t = I_n^t = I_n$. $\square$

9. (This is the Euclidean algorithm) Let $a, b \in \mathbb{Z}_{\geq 1}$ and consider the division with remainder $a = bq + r$, with $0 \leq r < b$.

   (a) Show that $(a, b) = (b, r)$.

   (b) Write $r_{-1} = a$ and $r_0 = b$ and define the sequence (r_n) recursively using division with remainder $r_{n-1} = r_nq_n + r_{n+1}$ with $0 \leq r_{n+1} < r_n$. Show that if $r_n > 0$ and $r_{n+1} = 0$ then $r_n = (a, b)$.

   Proof. (a): Suppose $d \mid a, b$. Then $d \mid r = a - bq$ and so $d \mid (b, r)$. If $d \mid b, r$ then $d \mid a = bq + r$ and so $d \mid (a, b)$. We conclude that $(a, b) = (b, r)$.

   (b): The sequence of residues $r_{-1} = a$, $r_0 = b > r_1 > r_2 > \ldots \geq 0$ must have a smallest positive entry $r_n > 0$ and $r_{n+1} = 0$. Then part (a) applied many times gives

$$(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = (r_n, 0) = r_n$$

   as the gcd between r_n and 0 is r_n. $\square$

10. (This is explicit Bezout. This seems elaborate but it really is straightforward and I recommend you do it.) Suppose $a, b \in \mathbb{Z}_{n\geq 1}$. We define the sequences (r_n), (q_n), (u_n) and (v_n) recursively as follows: $r_{-1} = a$, $r_0 = b$, and for $n \geq 0$ define q_{n+1} and r_{n+1} using the division with remainder $r_{n-1} = r_nq_{n+1} + r_{n+1}$ with $0 \leq r_{n+1} < r_n$. Also define $u_{-1} = 1$, $v_{-1} = 0$, $u_0 = 0$, $v_0 = 1$ and for $n \geq 0$

$$\begin{aligned} u_{n+1} &= u_{n-1} - q_{n+1}u_n \\ v_{n+1} &= v_{n-1} - q_{n+1}v_n \end{aligned}$$

   (a) Show that $r_n = au_n + bv_n$ by induction on n.

   (b) Show that $(a, b) = au_N + bv_N$ where N is the largest index such that $r_N > 0$. Here you may use the previous exercise whether or not you actually did it.

   (c) (Optional) Use this algorithm to find m and n such that $17m + 23n = 1$. [This is how a computer solves Bezout.]

   Proof. (a): We show this by induction. The base case is $r_{-1} = a = a\cdot 1 + b\cdot 0 = au_{-1} + bv_{-1}$ and $r_0 = b = 0\cdot a + 1\cdot b = u_0a + v_0b$.

   By definition $r_{n+1} = r_{n-1} - q_{n+1}r_n$. The inductive hypothesis is that $r_{n-1} = au_{n-1} + bv_{n-1}$ and $r_n = au_n + bv_n$ and so we deduce that

$$\begin{aligned} r_{n+1} &= r_{n-1} - q_{n+1}r_n \\ &= au_{n-1} + bv_{n-1} - q_{n+1}(au_n + bv_n) \\ &= a(u_{n-1} - q_{n+1}u_n) + b(v_{n-1} - q_{n+1}v_n) \\ &= au_{n+1} + bv_{n+1} \end{aligned}$$

   which yields the inductive step.

   (b): The previous exercise show that if N is the largest index such that $r_N > 0$ then $r_N = (a, b)$ and so from part (a) we deduce that $(a, b) = au_N + bv_N$.

   (c): Here is the result of the algorithm:

n	r_n	q_n	u_n	v_n
-1	23	–	1	0
0	17	–	0	1
1	6	1	1	-1
2	5	2	-2	3
3	1	1	3	-4
4	0	5		

which implies that $1 = (17, 23) = 17 \cdot (-4) + 23 \cdot 3$. $\square$