Math 30810 Honors Algebra 3
Homework 11

Andrei Jorza

Due at noon on Thursday, November 17

Do 8 of the following questions. Some questions are obligatory. Artin a.b.c means chapter a, section b, exercise c. You may use any problem to solve any other problem.

1. Let p be a prime, $G = \mathrm{GL}(n, \mathbb{F}_p)$ and U the subgroup of upper triangular matrices with 1-s on the diagonal.

   (a) Show that U is a p-Sylow subgroup.

   (b) Show that $N_G(U)$ is the group of upper triangular invertible matrices.

   (c) Determine n_p.

   Proof. (a): $|U| = p^{1+2+\cdots+(n-1)}$ while $|\mathrm{GL}(2, \mathbb{F}_p)| = (p^n - 1)(p^n - p)\cdots(p^n - p^{n-1})$ and the latter has largest power of p exactly $p^{1+2+\cdots+(n-1)}$. From a previous homework we already know that U was a group and thus it has to be a Sylow group.

   (b): Let A be the matrix with has 0-s under the diagonal and 1-s on and above the diagonal. If $X \in N_G(U)$ then $XAX^{-1} = B$ where $B \in U$ and so $XA = BX$. Look at the last row of the product. On the LHS this row is $x_{n,1}, x_{n,1} + x_{n,2}, \ldots, x_{n,1} + \cdots + x_{n,n}$ while on the RHS it is $x_{n,1}, x_{n,2}, \ldots, x_{n,n}$. We immediately deduce that $x_{n,1} = x_{n,2} = \ldots = x_{n,n-1} = 0$. Write $X = \begin{pmatrix} Y & Z \\ 0 & 1 \end{pmatrix}$ where $Y \in M_{n-1\times n-1}$ and $Z \in M_{n-1\times 1}$ and similarly write $A = \begin{pmatrix} A' & * \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} B' & * \\ 0 & 1 \end{pmatrix}$ where A', B' are upper triangular unipotent. Since $XA = BX$ this implies that (compare top left corners in the matrix products) that $YA' = B'Y$. Inductively we conclude that Y has to be upper triangular.

   (c): $n_p = |\mathrm{GL}(n, \mathbb{F}_p)|/|U| = \prod_{k=1}^{n} \dfrac{p^k - 1}{p - 1}$. □

2. Let R be a ring. An idempotent element of R is an element $e \in R$ such that $e^2 = e$. Consider $eR = \{ex \mid x \in R\}$. Show that $(eR, +_R, \cdot_R, 0_R, e)$ is a ring.

   Proof. $ex + 0 = 0 + ex = ex$ so 0 is a unit for $+$, $ex \cdot e = e \cdot ex = e^2x = ex$ so e is a unit for $\cdot$. Also $ex + ey = e(x + y)$ and $ex \cdot ey = exy$ so eR is closed under $+$ and $\cdot$. □

3. Show that $\mathbb{C}[x][\![y]\!] \neq \mathbb{C}[\![y]\!][x]$.

   Proof. The series $1 + xy + x^2y^2 + x^3y^3 + \cdots$ is in $\mathbb{C}[x][\![y]\!]$ but certainly not in $\mathbb{C}[\![y]\!][x]$ as the degree of x is unbounded. □

4. Suppose R is an integral domain ring with fraction field F (i.e., F is the smallest field containing R as a subring). What is the fraction field of $R[\![x]\!]$.

Proof. This was incorrectly stated in the original homework and the problem is not easy. We can chat about it if you want. □

5. Artin 9.5.6 on page 285. (A one-parameter group is a group of the form $\{e^{tA} \mid t \in \mathbb{R}\}$ where A is a matrix.)

Proof. Write $m(x,y) = \begin{pmatrix} x & \\ & x^{-1} \end{pmatrix}$. Then $m(a,b)m(x,y)m(a,b)^{-1} = m(x, a^2y + ab(x^{-1} - x))$. When $x \neq x^{-1}$, i.e., when $x \neq 1$, the map $b \mapsto a^2y + ab(x^{-1} - x)$ is surjective and so the conjugacy class of $m(x,y)$ is $m(x,*)$. Then $x = 1$, $m(a,b)m(1,y)m(a,b)^{-1} = m(1,a^2y)$ and so the conjugacy class of $m(1,y)$ is $\{I_2\}$ when $y = 0$, $\{m(1,>0)\}$ when $y > 0$ and $\{m(1,<0)\}$ when $y < 0$.
If $\{e^{tA} \mid t \in \mathbb{R}\} \subset G$ then $\det e^{tA} = e^{\operatorname{Tr} tA} = 0$ and so A has trace 0 which means that A has eigenvalues $\alpha, -\alpha$. If $\alpha \neq 0$ then A is diagonalizable so $A = SBS^{-1}$ with $B = \begin{pmatrix} \alpha & \\ & -\alpha \end{pmatrix}$ and S invertible. Then from a previous homework one has

$$e^{tA} = Se^{tB}S^{-1} = S \begin{pmatrix} e^{t\alpha} & \\ & e^{-t\alpha} \end{pmatrix} S^{-1}$$

and we have to figure out for what S the above formula is in G for all $t \in \mathbb{R}$.
Write $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. If $Se^{tB}S^{-1} \in G$ then $Se^{tB} = m(x,y)S$ for some x, y (which depend on t). Comparing the last row in the products yields $ce^{t\alpha}, de^{-t\alpha} = cx^{-1}, dx^{-1}$. If $c, d \neq 0$ then $x = e^{t\alpha} = e^{-t\alpha}$ but this can only happen when $t = 0$. We deduce that either $c = 0$ or $d = 0$. In both cases a simple computations yields that $Se^{tB}S^{-1} \in G$ always. This means that either

$$A = \begin{pmatrix} a & b \\ & d \end{pmatrix} \begin{pmatrix} \alpha & \\ & -\alpha \end{pmatrix} \begin{pmatrix} a & b \\ & d \end{pmatrix}^{-1} = \begin{pmatrix} \alpha & * \\ & -\alpha \end{pmatrix}$$

so A can be any upper triangular with trace 0 or

$$A = \begin{pmatrix} a & b \\ c & \end{pmatrix} \begin{pmatrix} \alpha & \\ & -\alpha \end{pmatrix} \begin{pmatrix} a & b \\ c & \end{pmatrix}^{-1} = \begin{pmatrix} -\alpha & * \\ & \alpha \end{pmatrix}$$

and again A can be any upper triangular with trace 0.
If $\alpha = 0$ then either $A = 0$ which certainly works or A has Jordan form $\begin{pmatrix} & 1 \\ & \end{pmatrix}$. If e^{tA} is a one parameter subgroup of G then for the invertible matrix S with $A = S \begin{pmatrix} & 1 \\ & \end{pmatrix} S^{-1}$ one must have that $S \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix} S^{-1} \in G$. But the lower left corner of this matrix is 0 for all values of $*$ if and only if $c = 0$. Again we get that A can be any upper triangular matrix with eigenvalues 0,0.
The final answer is A must be upper triangular with trace 0.

□

6. Suppose $A \in M_{n\times n}(\mathbb{R})$, $B \in \mathrm{GL}(n,\mathbb{R})$ and $x \in \mathbb{R}$. Recall from a previous homework that exponentials of matrices are always invertible. Compute

$$\frac{d}{dx}[e^{xA}, B]_{\mathrm{GL}(n)}|_{x=0}$$

where $[\cdot,\cdot]_{\mathrm{GL}(n)}$ is the usual group commutator in the group $\mathrm{GL}(n,\mathbb{R})$.

Proof. First note that $(e^{Ax})' = Ae^{Ax}$ simply by looking at the power series.
Now

$$\frac{d}{dx}e^{Ax}Be^{-Ax}B^{-1} = Ae^{Ax}Be^{-Ax}B^{-1} - e^{Ax}BAe^{-Ax}B^{-1}$$
$$\frac{d}{dx}e^{Ax}Be^{-Ax}B^{-1}|_{x=0} = A - BAB^{-1}$$

□

7. Let $A, B \in M_{n\times n}(\mathbb{R})$ and $x \in \mathbb{R}$. For general matrices write $[A, B] = AB - BA$. Show that

$$e^{xA}e^{xB} = e^{x(A+B)+x^2[A,B]/2+\text{higher order terms}}$$

[Hint: Write out the first terms of the Taylor series of $\log(e^{xA}e^{xB})$.]

Proof. Note that $(\log(f))' = \frac{f'}{f}$ while $(\log(f))'' = \frac{f''f - (f')^2}{f^2}$. Let $f = e^{Ax}e^{Bx}$. Then $f(0) = I_n$, $f'(0) = A + B$ and $f''(0) = A^2 + 2AB + B^2$. Thus $h = \log(f)$ has Taylor expansion

$$h(x) = h(0) + h'(0)x + h''(0)x^2/2 + O(x^3) = (A + B)x + [A, B]x^2/2 + O(x^3)$$

and so the result follows. □

8. Artin 11.1.6 on page 354.

Proof. (a): S is a subring. Indeed, $0 = 0/1$, $1 = 1/1$ and if $3 \nmid b, d$ then $3 \nmid bd$ in the fraction $a/b + c/d = (ad + bc)/(bd)$.
(b): S is not a subring. Indeed, $\sin t, \cos t \in S$ but their product is $\sin t \cos t = \sin(2t)/2$. If this product were in S then $\sin(2t)/2$ can be written as $a + \sum a_n \sin(nt) + \sum b_n \cos(nt)$ a finite sum with integer coefficients. Plugging in $\pi/4$ and collecting terms we'd get that $1/2 = a + b\sqrt{2}/2 + c$ with $a, b, c \in \mathbb{Z}$. But then $b = 0$ and $a + c = 1/2$ is not an integer. □

9. Artin 11.1.7 on page 354.

Proof. (a): This is a ring with $0 = \emptyset$ and $1 = U$. Then $A + 0 = 0 + A = A$ and $A \cdot 1 = 1 \cdot A = A$. Clearly $A + B = B + A$ and $AB = BA$ so we'd only need to check that $(A + B)C = AC + BC$. But

$$(A + B)C = (A \cup B - A \cap B) \cap C = (A \cup B) \cap C - A \cap B \cap C = (A \cap C) \cup (B \cap C) - A \cap B \cap C$$
$$= (A \cap C) \cup (B \cap C) - (A \cap C) \cap (B \cap C) = AC + BC$$

(b): Not a ring. Indeed, $f \circ g \neq g \circ f$ in general so the multiplication law is not commutative. □

10-11 (Counts as 2 problems) Artin 7.M.12 on page 228.

Proof. I'll do (c) and (d) as (a) and (b) simply follow from these. I'll do it for $p > 2$ as $\mathrm{SL}(2, \mathbb{F}_2) = \mathrm{GL}(2, \mathbb{F}_2) \cong S_3$ and you already know everything about S_3 anyway.
(a+c): Let's compute the centralizer of $A = \begin{pmatrix} & -1 \\ 1 & a \end{pmatrix}$. It consists of matrices X such that $XA = AX$ which, after a computation, is the set of matrices

$$C_{\mathrm{SL}(2,\mathbb{F}_p)}(A) = \{\begin{pmatrix} x & y \\ y & ay - x \end{pmatrix} \in \mathrm{SL}(2, \mathbb{F}_p)\} = \{\begin{pmatrix} x & y \\ y & ay - x \end{pmatrix} \mid x, y \in \mathbb{F}_p, x^2 - axy + y^2 = 1\}$$

This yields an answer to (a).

The equation $x^2 - axy + y^2 = 1$ always has the solutions $(0, \pm 1)$ and these are the only ones with $x = 0$. If (x, y) is any other solution then we can write $y = x\lambda + 1$ for some $\lambda \in \mathbb{F}_p$. Indeed, simply let $\lambda = (y-1)/x$. Setting aside the solutions $(0, \pm 1)$ we get the equation

$$x^2(1 - a\lambda + \lambda^2) = (a - 2\lambda)x$$

When $1 - a\lambda + \lambda^2 \neq 0$ then the only possibility is

$$x = \frac{a - 2\lambda}{1 - a\lambda + \lambda^2}$$

Each value of λ st $1 - a\lambda + \lambda^2 \neq 0$ yields one value of x and therefore one value of y. Note that if $\lambda = a/2 \in \mathbb{F}_p$ then we recover the solution $(0, 1)$.

When $1 - a\lambda + \lambda^2 = 0$, which can only happen if $a = u + 1/u$ for some $u \in \mathbb{F}_p^\times$ and $\lambda = u$ or $1/u$, then the equation becomes $0 = a - 2\lambda = u + 1/u - 2\lambda$ and this can happen (remember that $\lambda = u, 1/u$) iff $u = \pm 1$. When $a = u + 1/u$ with $u \neq \pm 1$ then $\lambda = u, 1/u$ yield NO solutions. When $u = \pm 1$, $a = u + 1/u = 2u$ then $\lambda = u = 1/u$ yields a solution for ANY value of x as the equation is satisfied for any value of x.

To recap:

- if a is not of the form $u + 1/u$ for some $u \in \mathbb{F}_p^\times$ then we get $p+1$ solutions to the equation as each value of λ yields a solution and $\lambda = a/2$ recovers $(0, 1)$, with $(0, -1)$ never counted by λ.
- if $a = u + 1/u$ for $u \in \mathbb{F}_p^\times - \{\pm 1\}$ then each $\lambda \neq u, 1/u$ yields a solution x and a solution y whereas $\lambda = u$ or $1/u$ yield no solutions. Adding in $(0, -1)$ we get a total of $p - 2 + 1 = p - 1$ solutions.
- if $a = u + 1/u$ with $u = \pm 1$ then each $\lambda \neq u = 1/u$ yields one solution x and one solution y but $\lambda = u$ yields p solutions for x, namely any value of x works. Finally we add $(0, -1)$ for a total of $p - 1 + p + 1 = 2p$ solutions.

(d): Let $e \in \mathbb{F}_p^\times$ such that $-e \notin \{x^2 \mid x \in \mathbb{F}_p^\times\}$. Since the map $x \mapsto x^2$ is a group homomorphism with kernel ± 1 it follows that its image has size $(p-1)/2$ and so we can choose such an e when $p > 2$. I claim that the conjugacy classes of $\mathrm{SL}(2, \mathbb{F}_p)$ have representatives $\pm I_2$, $\begin{pmatrix} 1 & e \\ & 1 \end{pmatrix}$, $\begin{pmatrix} -1 & e \\ & -1 \end{pmatrix}$ and $\{\begin{pmatrix} & -1 \\ 1 & a \end{pmatrix} \mid a \in \mathbb{F}_p\}$ for a total of $p + 4$ conjugacy classes. The scalar matrices have trivial conjugacy classes so to check that the other matrices are in different conjugacy classes we look at their characteristic polynomials as conjugate matrices have the same characteristic polynomials. note that their characteristic polynomials are $(X \pm 1)^2$ and $X^2 - aX + 1$ which are all distinct unless $a = \pm 2$. When $a = 2$ for example (the case $a = -2$ is analogous) then $\begin{pmatrix} & -1 \\ 1 & 2 \end{pmatrix}$ has the same characteristic polynomial as $\begin{pmatrix} 1 & e \\ & 1 \end{pmatrix}$. But these two matrices can be conjugate only by a matrix of the form $S = \begin{pmatrix} u & v \\ -u & -ue - v \end{pmatrix}$ and this is in $\mathrm{SL}(2, \mathbb{F}_p)$ iff the determinant is $-u^2 e = 1$. But then $-e$ would be a perfect square in $\mathbb{F}_p^\times$ contradicting its choice.

Recall that the conjugacy class of g has $|G/C_G(g)|$ elements. The scalar matrices have trivial conjugacy classes. The matrices $\begin{pmatrix} \varepsilon & e \\ & \varepsilon \end{pmatrix}$ where $\varepsilon = \pm 1$ have centralizers $\{\pm \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}\}$ so the centralizers have size $2p$.

Note that the map $f(u) = u + 1/u : \mathbb{F}_p^\times \to \mathbb{F}_p$ sends 1 to 2, -1 to -2 and is two-to-one on $\mathbb{F}_p^\times - \{\pm 1\}$. Therefore its image has size $2 + (p-3)/2 = (p+1)/2$ with complement of size $(p-1)/2$. When $a \notin \mathrm{Im}\, f$

we get centralizers of size $p+1$ from part (c). When $a = \pm 2$ we get centralizers of size $2p$ and when $a \in \operatorname{Im} f - \{\pm 2\}$ we get centralizers of size $p-1$. The total cardinality of these $p+4$ conjugacy classes is

$$\underbrace{2}_{\pm I_2} + \underbrace{2 \cdot \frac{p^3-p}{2p}}_{\begin{pmatrix} \varepsilon & e \\ & \varepsilon \end{pmatrix}} + \underbrace{\frac{p-3}{2} \cdot \frac{p^3-p}{p-1}}_{a \in \operatorname{Im} f - \{\pm 2\}} + \underbrace{2 \cdot \frac{p^3-p}{2p}}_{a = \pm 2} + \underbrace{\frac{p-1}{2} \cdot \frac{p^3-p}{p+1}}_{a \notin \operatorname{Im} f} = p^3 - p = |\operatorname{SL}(2, \mathbb{F}_p)|$$

and therefore these $p+4$ conjugacy classes exhaust all of $\operatorname{SL}(2, \mathbb{F}_p)$ and the above formula is the class equation. $\square$