EXERCISES FOR WEEK 4

AURÈE GUILLEVIC

Exercises

Exercise 1 (3.4). Let $M$ and $N$ be $2 \times 2$ matrices with $N = \begin{pmatrix} w & x \\ y & z \end{pmatrix}$. Define $\tilde{N} = \begin{pmatrix} z & -x \\ -y & w \end{pmatrix}$ (this is the adjoint matrix).

(a) Show that $\text{Trace}(M \tilde{N}) = \det(M + N) - \det(M) - \det(N)$.
(b) Use 1 to show that
\[
\det(aM + bN) = a^2 \det(M) - b^2 \det(N) = ab(\det(M + N) - \det(M) - \det(N))
\]
for all scalars $a, b$. This is the relation used in the proof of Proposition 3.16.

Solution 1. Let $M = \begin{pmatrix} i & j \\ k & l \end{pmatrix}$.

(a) The trace of a matrix is the sum of the diagonal coefficients. Let’s compute $M \tilde{N}$:
\[
M \tilde{N} = \begin{pmatrix} i & j \\ k & l \end{pmatrix} \begin{pmatrix} z & -x \\ -y & w \end{pmatrix} = \begin{pmatrix} iz - jy & -ix + jw \\ kz - ly & -kx + lw \end{pmatrix}
\]
The trace is $\text{Trace}(M \tilde{N}) = iz - jy - kx + lw$.

Now compute $M + N$, this is
\[
M + N = \begin{pmatrix} i & j \\ k & l \end{pmatrix} \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} i + w & j + x \\ k + y & l + z \end{pmatrix}
\]
and the determinant is $\det(M + N) = (i+w)(l+z) - (j+y)(j+x) = il+iz+wl+wz-jk-kx-jy-xy$.

Then $\det(M) = il - jk$ and $\det(N) = wz - xy$, and $\det(M + N) - \det(M) - \det(N) = iz + wl - kx - jy = \text{Trace}(M \tilde{N})$ as wanted.

\texttt{Raz.<a,b,i,j,k,l,w,x,y,z>=QQ[]} \n\texttt{M = Matrix(Raz, 2, 2, [i,j,k,l])} \n\texttt{N = Matrix(Raz, 2, 2, [w,x,y,z])} \n\texttt{N.adjugate()} \n\texttt{(M * N.adjugate()).trace() == (M+N).det() - M.det() - N.det()} \n\# l*w - k*x - j*y + i*z

(b) $\det(aM) = a^2 \det(M)$, $\det(bN) = b^2 \det(N)$, $\det(aM+bN) = \det(aM) - \det(bN) = \text{Trace}(aMb\tilde{N})$, where $aMb\tilde{N} = ab(M\tilde{N})$, so that $\text{Trace}(aMb\tilde{N}) = \text{Trace}(ab(M\tilde{N})) = ab \text{Trace}(M\tilde{N}) = ab(\det(M + N) - \det(M) - \det(N))$ by linearity of the trace.

\texttt{((a*M) * (b*N).adjugate()).trace() == (a*M+b*N).det() - (a*M).det() - (b*N).det()} \n\# a*b*l*w - a*b*k*x - a*b*j*y + a*b*i*z

Exercise 2. Consider the elliptic curves
\[ E: y^2 = x^3 + x \text{ over } \mathbb{F}_p \text{ where } p \geq 5 \text{ and with } p \equiv 3 \text{ mod } 4. \]

Prove that the order of the curves is $p + 1$.

Hint: For $E_+: y^2 = x^3 + x$, define the three sets
\[ S_1 = \{x \in \mathbb{F}_p, \ x^3 + x \text{ is a non-zero square} \}, \]
\[ S_2 = \{x \in \mathbb{F}_p, \ x^3 + x = 0 \}, \]
\[ S_3 = \{x \in \mathbb{F}_p, \ x^3 + x \text{ is not a square} \}. \]

\textit{Date:} Week 4.
What can you say about the curve order in terms of the orders of $S_1, S_2, S_3$? What can you say about the order of $S_1$ with respect to the order of $S_3$? Consider $x^3 - x$ instead of $x^3 + x$ for the second curve.

**Solution 2.** For each $x \in S_1$, there are two distinct points $(x, y), (x, -y)$ on the curve. For each $x \in S_3$, there is no point on the curve. For each $x \in S_2$, there is one point on the curve. Then
\[
\#E(F_p) = 2\#S_1 + S_2 + \#\{O\} = 2\#S_1 + S_2 + 1.
\]
Besides, the three sets are a partition of $\{0, 1, \ldots, p - 1\}$ that is,
\[
\#S_1 + \#S_2 + \#S_3 = \#F_p = p.
\]
We observe that the sets $S_1$ and $S_3$ are in bijection through the map $x \mapsto -x$, indeed, let $x \in S_1$, so that
\[
x^3 + x \text{ is a square. Then } (-x)^3 + (-x) = -(x^3 + x) \text{ is not a square because } (-1) \text{ is not a square in } F_p,
\]
and $-x \notin S_1, -x \in S_3$. Note that $S_1 \cap S_3 = \emptyset$ and that $0 \notin S_1, 0 \notin S_3$. Hence
\[
\#S_1 = \#S_3
\]
and from $\#S_1 + \#S_2 + \#S_3 = p$ we obtain $2\#S_1 + \#S_2 = p$. Finally $\#E(F_p) = 2\#S_1 + \#S_2 + 1 = p + 1$.

**Exercise 3.** Consider the elliptic curve

\[
E: y^2 = x^3 + b \text{ over } F_p \text{ where } b \neq 0, \ p \geq 5 \text{ and with } p \equiv 2 \mod 3.
\]
Prove that the order of the curve is $p + 1$.

- **Hint:** In a prime finite field $F_p$ with $p \equiv 2 \mod 3$, the order of the multiplicative subgroup $F_p^*$ is $p - 1$ and observe that $3 \nmid p - 1$ ($3$ does not divide $p - 1$). There is no subgroup of order $3$, and the kernel of the endomorphism $x \mapsto x^3$ in $F_p^*$ is $\{1\}$. It means that any non-zero element of $F_p^*$ has exactly one cube root. Moreover $x^3 = 0$ has one root $x = 0$, so finally, $x^3 = c$ has only one root for any $c \in F_p$.

- Rewrite the curve equation as
\[
E: y^2 - b = x^3.
\]
Consider the pairs $(y, -y)$ of opposite $y$-coordinates, with $y 
eq 0$ so that $y \neq -y$. How many pairs are they? How many solutions $x \in F_p$ are they for each pair $(y, -y)$?

- Consider $y = 0$ separately.

**Solution 3.** There are $(p - 1)/2$ pairs of opposite distinct $y$-coordinates $(y, -y)$ in $F_p$. For each pair $(y, -y)$, there is exactly one $x \in F_p$ satisfying $x^3 = y^2 - b = (-y)^2 - b$, and we have two points $(x, y)$ and $(x, -y)$. That makes $p - 1$ points. For $y = 0$, there is one point $(\sqrt[3]{-b}, 0)$. Finally there is the point at infinity, that makes $p + 1$ points.

_E-mail address: aurore.guillevic@inria.fr_