EXERCISES FOR WEEK 4

AURORE GUILLEVIC

Exercises

Exercise 1 (3.4)**.** Let M and N be 2×2 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 $\mathrm{Trace}(M\tilde{N}) = \det(M+N) - \det(M) - \det(N)$.

(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 $\mathrm{Trace}(M\tilde{N}) = iz - jy - kx + lw$.

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 $\det(M+N) = (i+w)(l+z) - (k+y)(j+x) = il + iz + wl + wz - jk - kx - jy - xy$. Then $\det(M) = il - jk$ and $\det(N) = wz - xy$, and $\det(M+N) - \det(M) - \det(N) = iz + wl - kx - jy = \mathrm{Trace}(M\tilde{N})$ as wanted.

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

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

```
((a*M) * (b*N).adjugate()).trace() == (a*M+b*N).det() - (a*M).det() - (b*N).det()
# a*b*l*w - a*b*k*x - a*b*j*y + a*b*i*z
((a*M) + (b*N)).det() - a^2*M.det() - b^2 * N.det() == a*b*((M+N).det()-M.det()-N.det())
# True
```

Exercise 2. Consider the elliptic curves

$$E\colon y^2 = x^3 \pm x \text{ over } \mathbb{F}_p \text{ where } p \geq 5 \text{ and with } p \equiv 3 \bmod 4 \,.$$

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

Hint: For $E_+ \colon y^2 = x^3 + x$, Define the three sets

$$\begin{aligned} S_1 =& \{x \in \mathbb{F}_p,\ x^3 + x \text{ is a non-zero square}\}, \\ S_2 =& \{x \in \mathbb{F}_p,\ x^3 + x = 0\}, \\ S_3 =& \{x \in \mathbb{F}_p,\ x^3 + x \text{ is not a square}\}. \end{aligned}$$

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

$$\#E(\mathbb{F}_p) = 2\#S_1 + S_2 + \#\{\mathcal{O}\} = 2\#S_1 + S_2 + 1 \ .$$

Besides, the three sets are a partition of $\{0, 1, \ldots, p-1\}$ that is,

$$\#S_1 + \#S_2 + \#S_3 = \#\mathbb{F}_p = p \ .$$

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 $x^3 + x$ is a square. Then $(-x)^3 + (-x) = -(x^3 + x)$ is not a square because (-1) is not a square in $\mathbb{F}_p$, 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 $\#E(\mathbb{F}_p) = 2\#S_1 + \#S_2 + 1 = p + 1$.

Exercise 3. Consider the elliptic curve

$$E\colon y^2 = x^3 + b \text{ over } \mathbb{F}_p \text{ where } b \neq 0,\ p \geq 5 \text{ and with } p \equiv 2 \bmod 3 \ .$$

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

Hint: In a prime finite field $\mathbb{F}_p$ with $p \equiv 2 \bmod 3$, the order of the multiplicative subgroup $\mathbb{F}_p^*$ 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 $\mathbb{F}_p^*$ is $\{1\}$. It means that any non-zero element of $\mathbb{F}_p^*$ 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 $c \in \mathbb{F}_p$.

Rewrite the curve equation as

$$E\colon y^2 - b = x^3 \ .$$

Consider the pairs $(y, -y)$ of opposite y-coordinates, with $y \neq 0$ so that $y \neq -y$. How many pairs are they? How many solutions $x \in \mathbb{F}_p$ 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 $\mathbb{F}_p$. For each pair $(y, -y)$, there is exactly one $x \in \mathbb{F}_p$ 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`