

Random Exercises

Patricio Quiroz

Wesleyan University 2014

1. (*Reading L'arithmetique dans les algebres de matrices*) Show that a matrix algebra is regular (i.e. non invertible elements are zero divisors).

Proof. Let A be a non invertible matrix. By row and column operations, we can

write $E_1AE_2 = \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix}$, where E, E' are invertible matrices and at

least $a_n = 0$. Since $\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix} \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b \end{pmatrix} = 0$ for $b \neq 0$, we have

that E_1AE_2 is a zero divisor. Now, $E_1AE_2B = 0$ implies $AE_2B = 0$ (same reasoning for $BE_1AE_2 = 0$). Hence A is a zero divisor.

2. (*Talking with Gabriel*) Show that $\text{Hom}_{\mathbb{Z}_{(p)}}(\mathbb{Z}_p, \mathbb{Z}_p) \cong \mathbb{Z}_p$.

Proof. We show first that $\text{Hom}_{\mathbb{Z}_{(p)}}(\mathbb{Z}_p, \mathbb{Z}_p) = \text{Hom}_{\mathbb{Z}_{(p)}}^c(\mathbb{Z}_p, \mathbb{Z}_p)$. Let $f \in \text{Hom}_{\mathbb{Z}_{(p)}}(\mathbb{Z}_p, \mathbb{Z}_p)$.

It is enough to prove continuity at $x = 0$. So, by taking $x = up^n \in \mathbb{Z}_p$ we have $f(x) = p^n f(u)$. Here n big implies $|f(x)|_p = \frac{|f(u)|_p}{p^n} \leq \frac{1}{p^n}$ small.

Now we prove what we really want to. Let ϕ be the map $\phi : \mathbb{Z}_p \rightarrow \text{Hom}_{\mathbb{Z}_{(p)}}(\mathbb{Z}_p, \mathbb{Z}_p)$

given by $\phi(a) : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$, $\phi(a)(x) = ax$. This is clearly an injective homomorphism.

Now, we prove that ϕ is onto. Let $f \in \text{Hom}_{\mathbb{Z}_{(p)}}(\mathbb{Z}_p, \mathbb{Z}_p)$. Since $\mathbb{Z}_{(p)}$ is dense in \mathbb{Z}_p and f is continuous we have $f(x) = \lim f(x_n)$, where $\{x_n\} \subset \mathbb{Z}_{(p)}$ converges to x .

Hence, $f(x) = f(1) \lim x_n = f(1)x$.

3. (*Hyperbolic Geometry course, we needed quaternion division algebras in order to produce Fuchsian groups*) Let $\left(\frac{a,p}{\mathbb{Q}}\right)$ be a quaternion algebra such that $\left(\frac{a}{p}\right) = -1$. Then $\left(\frac{a,p}{\mathbb{Q}}\right)$ is a division algebra.

Proof. We know that $\left(\frac{a,p}{\mathbb{Q}}\right)$ is a division algebra if and only if the norm form $\langle 1 \rangle \perp \langle -a \rangle \perp \langle -p \rangle \perp \langle ap \rangle$ is isotropic. Let $x, y, z, w \in \mathbb{Z}$ such that $x^2 - ay^2 - pz^2 + apw^2 = 0$ or, equivalently, $x^2 - ay^2 + apw^2 = pz^2$. Reducing mod p implies $x^2 \equiv ay^2 \pmod{p}$, which implies that $p|y$ since a is not a square mod p . This in turn implies

$p|x$. Now, looking at the equation mod p^2 we get $apw^2 = pz^2 \pmod{p^2}$ which implies that $aw^2 = z^2 \pmod{p}$ and then $p|w, p|z$. The result follows by descent (you get the same equation replacing x by $\frac{x}{p}$, etc.)

4. (For exercise 8 c), chapter 4, Marcus book "Number Fields") Take $x \equiv 1 \pmod{e}$, $x \equiv m \pmod{q}$ (it can be done by Chinese Remainder Theorem). Now we need a prime $p \equiv x \pmod{eq}$. If $(x, eq) = 1$ we can pick p from the arithmetic progression $a_n = x + eq \cdot n$. The first congruence implies $(x, e) = 1$ and the second one implies $(x, q) = 1$. Hence, $(x, eq) = 1$ since $q \nmid e$.

5. (Dando jugo) Prove that there is no integer between two consecutive integers.

Proof. If x were an integer between two consecutive integers, we would have, after translation, that $1 < x < 2$. Now, $x = \prod p_i^{\alpha_i}$, where $\alpha_i \geq 0$ and $p_i \geq 2$ for all i . This gives us a contradiction.