MODULAR REPRESENTATIONS OF $\mathrm{GL}_2(\mathbf{F}_p)$

LAURENT BERGER AND SANDRA ROZENSZTAJN

The goal of this project is to study certain *representations* of the group $\mathrm{GL}_2(\mathbf{F}_p)$ of invertible 2×2 matrices with coefficients in the field with p elements $\mathbf{F}_p$, where p is a prime number.

1. The group $\mathrm{GL}_2(\mathbf{F}_p)$ and its subgroups

Let $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. Let $\mathrm{M}_2(\mathbf{F}_p)$ denote the set of 2×2 matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with a, b, c and d in $\mathbf{F}_p$. Let $\mathrm{Id} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. If $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, let $\det(M) = ad - bc$. We say that M is *invertible* if there exists $N \in \mathrm{M}_2(\mathbf{F}_p)$ such that $MN = \mathrm{Id}$.

Exercise 1. *Check that* $\det(MN) = \det(M)\det(N)$, *compute* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \times \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$, *and prove that* M *is invertible if and only if* $\det(M) \neq 0$.

We let $\mathrm{GL}_2(\mathbf{F}_p)$ denote the set of matrices $M \in \mathrm{M}_2(\mathbf{F}_p)$ such that $\det(M) \neq 0$, and $\mathrm{SL}_2(\mathbf{F}_p)$ denote the set of matrices $M \in \mathrm{M}_2(\mathbf{F}_p)$ such that $\det(M) = 1$.

Exercise 2. *Prove that* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbf{F}_p)$ *belongs to* $\mathrm{GL}_2(\mathbf{F}_p)$ *if and only if* $\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right)$ *and* $\left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right)$ *is not a multiple of* $\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$. *Use this to show that* $|\mathrm{GL}_2(\mathbf{F}_p)| = (p^2-1)(p^2-p)$ *and that* $|\mathrm{SL}_2(\mathbf{F}_p)| = p(p^2-1)$.

Exercise 3 (Exceptional isomorphisms)**.** *Let* S_n *denote the permutation group of* $\{1, 2, \ldots, n\}$.

1. *Exercise 2 implies that* $|\mathrm{GL}_2(\mathbf{F}_2)| = 6$. *How many groups of cardinal* 6 *do you know?*
2. *There are* 3 *nonzero points in* $\mathbf{F}_2^2$. *The action of* $\mathrm{GL}_2(\mathbf{F}_2)$ *on those points gives rise to a map* $\mathrm{GL}_2(\mathbf{F}_2) \to S_3$. *Prove that this map is an isomorphism.*
3. *Likewise,* $|\mathrm{GL}_2(\mathbf{F}_3)| = 48$. *There are* 4 *lines in* $\mathbf{F}_3^2$. *Use this to show that there is a surjective map* $\mathrm{GL}_2(\mathbf{F}_3) \to S_4$, *whose kernel is* $\{\mathrm{Id}, -\mathrm{Id}\}$.
4. *(more difficult) Find a surjective map* $\mathrm{GL}_2(\mathbf{F}_5) \to S_5$.
5. *In each of the above, what is the image of* $\mathrm{SL}_2(\mathbf{F}_p)$*?*

Let $\mathrm{Z} = \{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \text{ with } a \in \mathbf{F}_p^\times\}$.

Exercise 4. *Prove that* Z *is the* center *of* $\mathrm{GL}_2(\mathbf{F}_p)$.

Exercise 5. *Prove that there exists $g \in \mathbf{F}_p^\times$ such that $\mathbf{F}_p^\times = \{1, g, \dots, g^{p-2}\}$. Show that every multiplicative map $f : \mathbf{F}_p^\times \to \mathbf{F}_p^\times$ is of the form $x \mapsto x^r$, with $0 \leq r \leq p-2$.*

Let B denote the set of upper triangular matrices $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ that belong to $\mathrm{GL}_2(\mathbf{F}_p)$. Let U be the set of matrices of the form $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ for $a \in \mathbf{F}_p$. Let $w = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

Exercise 6. *Prove that every multiplicative map $f : \mathrm{B} \to \mathbf{F}_p^\times$ is of the form $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \mapsto a^r \cdot d^s$ with $0 \leq r, s \leq p-2$.*

Exercise 7 (Bruhat decomposition)**.** *Show that $\mathrm{GL}_2(\mathbf{F}_p) = \mathrm{B} \cup \mathrm{U}w\mathrm{B}$, and more precisely that $\mathrm{GL}_2(\mathbf{F}_p)$ is the disjoint union of B and of the $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right) w\mathrm{B}$ for $a \in \mathbf{F}_p$.*

Exercise 8. *Prove that every multiplicative map $f : \mathrm{G} \to \mathbf{F}_p^\times$ is of the form $M \mapsto \det(M)^r$ for some $0 \leq r \leq p-2$.*

Hint: use exercise 6 and compute $w \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) w$. Show that $r = s$, so that $f = \det^r$ on B, then use exercise 7.

Another method would be to prove that f is trivial on $\mathrm{SL}_2(\mathbf{F}_p)$ because $\mathrm{SL}_2(\mathbf{F}_p)$ is the derived group *of $\mathrm{GL}_2(\mathbf{F}_p)$ – at least if $p \geq 5$, see* [Lan02, §8, XIII]*, and $\det : \mathrm{GL}_2(\mathbf{F}_p)/\mathrm{SL}_2(\mathbf{F}_p) \to \mathbf{F}_p^\times$ is an isomorphism.*

2. Representations of groups

Let E be a field, and let V be an E-vector space. The space $\mathrm{End}(V)$ is the set of E-linear maps $f : V \to V$, and $\mathrm{Aut}(V)$ is the set of maps $f \in \mathrm{End}(V)$ that are invertible.

If G is a group, a *representation* of G is a group homomorphism $\rho_V : G \to \mathrm{Aut}(V)$. In other words, for every $g \in \mathrm{G}$, the map $\rho_V(g) : V \to V$ is E-linear and invertible, and $\rho_V(gh) = \rho_V(g)\rho_V(h)$ if g, $h \in \mathrm{G}$ and $\rho_V(1) = \mathrm{Id}$.

A *subrepresentation* of V is a subspace W of V such that W is stable under $\rho_V(g)$ for all $g \in \mathrm{G}$. Let V^{G} be the set of $v \in V$ such that $\rho_V(g)(v) = v$ for all $g \in \mathrm{G}$. This is a subrepresentation of V. We say that V is *irreducible* if $V \neq \{0\}$, and the only subrepresentations of V are $\{0\}$ and V itself.

If V and W are two representations of G, then a *morphism of representations*, also called an *intertwining operator*, is a linear map $f : V \to W$ such that $f(\rho_V(g)(v)) = \rho_W(g)(f(v))$ for all $g \in \mathrm{G}$ and $v \in V$.

In all of this project, G is a finite group, E is a finite field, and V is a finite dimensional E-vector space. For example: let $E = \mathbf{F}_p$ for some prime number p, let S_n be the permutation group of $\{1, \dots, n\}$ and let $V = Ee_1 \oplus \cdots Ee_n$. If $g \in S_n$, we define $\rho_V(g) : V \to V$ by requiring that $\rho_V(g)(e_i) = e_{g(i)}$.

Exercise 9. *Check that V defined above is a representation of S_n. Let $W = \{\sum_{i=1}^n x_i e_i$ such that $\sum_{i=1}^n x_i = 0\}$ and let $X = E(e_1 + \cdots + e_n)$.*

(1) *Show that W and X are both subrepresentations of V, and that $X = V^{S_n}$.*
(2) *Show that if $n \neq 0$ in E, then $W \oplus X = V$.*
(3) *If $n = p$, is there a subrepresentation Y of V such that $W \oplus Y = V$?*
(4) *Is W an irreducible representation in general?*

If $v \in V$, the *orbit* of v is the set $\mathrm{Orb}(v) = \{\rho_V(g)(v)\}_{g \in \mathrm{G}}$. Let G_v be the set of $g \in \mathrm{G}$ such that $\rho_V(g)(v) = v$.

Exercise 10. *Let G be a finite group and let $V \neq \{0\}$ be a representation of G on a finite dimensional $\mathbf{F}_p$-vector space.*

(1) *Prove that G_v is a subgroup of G, and that $|\mathrm{Orb}(v)| = |\mathrm{G}|/|\mathrm{G}_v|$.*
(2) *Assume now that $|\mathrm{G}|$ is a power of p. Show that $|\mathrm{Orb}(v)|$ is of the form p^e with $e \geq 0$, and use this to prove that $V^{\mathrm{G}} \neq \{0\}$.*

The fact that $V^{\mathrm{G}} \neq \{0\}$ for any nonzero $\mathbf{F}_p$-representation of a *p-group* G is a fundamental result of the theory of $\mathbf{F}_p$-representations.

3. Irreducible constituents

If V is a representation of G and W is a subrepresentation of V, then the quotient space V/W is a representation of G.

Exercise 11. *Check that if $V \neq \{0\}$ is a finite dimensional representation of G, then it has an irreducible subrepresentation.*

Let V be a finite dimensional nonzero representation of G, and define the multiset $\mathrm{Irr}(V)$ as follows. If V is irreducible, then $\mathrm{Irr}(V) = \{V\}$. Otherwise, let W be an irreducible subrepresentation of W, and let $\mathrm{Irr}(V) = \{W\} \cup \mathrm{Irr}(V/W)$.

The *Jordan-Hölder theorem* says that the set $\mathrm{Irr}(V)$ does not depend on the choice of an irreducible representation at each step: they all arise in some order. The set $\mathrm{Irr}(V)$ is the set of *irreducible constituents* of V, and the cardinality of $\mathrm{Irr}(V)$ is the *length* of V. You can find a proof of the Jordan-Hölder theorem in §13 of [CR06], for instance.

Exercise 12. *Prove the Jordan-Hölder theorem for representations of length* 2.

Exercise 13 (Maschke's theorem)**.** *(more difficult and not used in the sequel) Prove that if $|\mathrm{G}| \neq 0$ in E, and V is a finite-dimensional representation of G, then $V = \oplus_{X \in \mathrm{Irr}(V)} X$.*

Hint: if W is a subrepresention of V, let π be a projector on V whose image is W. Let $\sigma = (\sum_{g \in \mathrm{G}} \rho_V(g) \pi \rho_V(g)^{-1})/|G|$. Prove that $\sigma|_W = \mathrm{Id}$, that σ is also a projector on V whose image is W, and that its kernel is stable under the action of G.

Item (3) of exercise 9 shows that this fails if $|\mathrm{G}| = 0$ in E. Here is a simpler example: let $E = \mathbf{F}_p$ and $\mathrm{G} = \mathbf{Z}/p\mathbf{Z}$ and let $V = Ex \oplus Ey$, with $\rho_V(g)(x) = x$ and $\rho_V(g)(y) = y + gx$.

Exercise 14. *Check that* $\mathrm{Irr}(V) = \{E, E\}$ *but that* $V \neq E^2$ *(here E denotes the one-dimensional representation of* G, *with* G *acting trivially).*

4. The representations Pol_k

Let $E = \mathbf{F}_p$. Take $k \geq 0$ and let Pol_k be the space of homogenous polynomials of degree k in two variables x and y, so that $\mathrm{Pol}_k = Ex^k \oplus Ex^{k-1}y \oplus \cdots \oplus Ey^k$. If $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{F}_p)$ and $P(x, y) \in \mathrm{Pol}_k$, let $(\rho_{\mathrm{Pol}_k}(g) \cdot P)(x, y) = P(ax + cy, bx + dy)$. If $r \in \mathbf{Z}$, let $\mathrm{Pol}_k(r)$ denote the same space of polynomials, but with the action of $\mathrm{GL}_2(\mathbf{F}_p)$ given by $(\rho_{\mathrm{Pol}_k(r)}(g) \cdot P)(x, y) = P(ax + cy, bx + dy) \cdot \det(g)^r$. One of the main goals of this project is to prove the following theorem.

Theorem 1. *The representations* $\mathrm{Pol}_k(r)$ *for* $0 \leq k \leq p-1$ *are all irreducible, and moreover every irreducible representation of* $\mathrm{GL}_2(\mathbf{F}_p)$ *is of the form* $\mathrm{Pol}_k(r)$ *for some* $0 \leq k \leq p-1$ *and* $0 \leq r \leq p-2$.

This theorem first appears in §30 of [BN41], with a proof that is very different from the one that we will see in this project.

Exercise 15. *Prove that if V is an irreducible representation of* $\mathrm{GL}_2(\mathbf{F}_p)$, *there exists* $0 \leq r \leq p-2$ *such that* $\rho_V(z) = \det(z)^r \cdot \mathrm{Id}$ *if* $z \in \mathrm{Z}$.

The character $\det^r : \mathrm{Z} \to \mathbf{F}_p^\times$ attached to V is called the *central character* of V. If V is a representation of $\mathrm{GL}_2(\mathbf{F}_p)$ that is not necessarily irreducible, we say that V has a central character if there is an r such that $\rho_V(z) = \det(z)^r \cdot \mathrm{Id}$ for all $z \in \mathrm{Z}$, and we then call the character $\det^r : \mathrm{Z} \to \mathbf{F}_p^\times$ the central character of V.

Exercise 16. *Does* $\mathrm{Pol}_k(r)$ *have a central character? Show that two representations* $\mathrm{Pol}_k(r)$ *and* $\mathrm{Pol}_{k'}(r')$ *are isomorphic if and only if* $k = k'$ *and* $p-1$ *divides* $r - r'$.

Exercise 17. *Show that the representations listed in Theorem 1 are indeed irreducible.*

Hint: Compute $(\mathrm{Pol}_k(r))^{\mathrm{U}}$, *and use exercise 10.*

At this point we have found $p(p-1)$ pairwise non-isomorphic irreducible representations of $\mathrm{GL}_2(\mathbf{F}_p)$. We want to show that every irreducible representation is isomorphic to one of these. First we show that the $\mathrm{Pol}_k(r)$ are not irreducible for $k \geq p$.

Exercise 18. *Show that* $\mathrm{Pol}_p(r)$ *contains a subrepresentation that is isomorphic to* $\mathrm{Pol}_1(r)$*.*

Let $D(x,y) = x^p y - xy^p$.

Exercise 19. *Compute* $D(ax+cy, bx+dy)$ *and prove that* $\mathrm{Pol}_k(r)$ *is not irreducible if* $k \geq p$*.*

5. Construction of representations

Let V be a representation of G, and let V^* be the *dual vector space*, the space of linear maps $\mu : V \to E$. We make V^* into a representation of G by setting $\rho_{V^*}(g)(\mu)(x) = \mu(\rho_V(g^{-1})(x))$ for all $\mu \in V^*$ and $x \in V$. This is called the *contragredient* representation of V.

Exercise 20. *Show that* V *is an irreducible representation of* G *if and only if* V^* *is.*

Exercise 21. *Show that the representation* $\mathrm{Pol}_k(r)^*$ *is isomorphic to* $\mathrm{Pol}_k(-r-k)$*.*

Recall that G is a finite group. Let H be a subgroup of G and let V be a representation of H. We define the *induced representation* $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}} V$ to be the set of maps $f : \mathrm{G} \to V$ satisfying the property: for all $h \in \mathrm{H}$ and $g \in \mathrm{G}$, $f(hg) = \rho_V(h)(f(g))$. We make this vector space into a representation of G by setting $\rho_{\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}} V}(g)(f)(x) = f(xg)$.

Exercise 22. *Check that* $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}} V$ *is indeed a representation of* G*. What is its dimension?*

Exercise 23 (Frobenius reciprocity)**.** *Let* G *be a finite group and* H *be a subgroup of* G *and* V *be an* $\mathbf{F}_p$*-representation of* G*. Let* W *be an irreducible representation of* H*. Suppose that* $V|_{\mathrm{H}}$ *contains a subrepresentation isomorphic to* W*. Show that there is a nonzero map* $\mathrm{Ind}_{\mathrm{H}}^{\mathrm{G}} W \to V$*, which is a morphism of representations of* G*.*

6. Parabolic induction

Let χ be a multiplicative map $\mathrm{B} \to \mathbf{F}_p^\times$, which gives rise to a one-dimensional representation of B. Let $\mathrm{ind}_{\mathrm{B}}^{\mathrm{GL}_2(\mathbf{F}_p)} \chi$ be the induced representation (see exercise 22; in this case, it is called a *parabolic induction*).

Exercise 24. *Show that* $\mathrm{ind}_{\mathrm{B}}^{\mathrm{GL}_2(\mathbf{F}_p)} \chi$ *is a vector space of dimension* $p+1$*.*

Exercise 25. *Show that the contragredient representation* $(\mathrm{ind}_{\mathrm{B}}^{\mathrm{GL}_2(\mathbf{F}_p)} \chi)^*$ *is isomorphic to* $\mathrm{ind}_{\mathrm{B}}^{\mathrm{GL}_2(\mathbf{F}_p)} (\chi^{-1})$*.*

Denote by $\chi(r,s)$ the multiplicative map $\mathrm{B} \to \mathbf{F}_p^\times$ of exercise 6, which is given by $\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \mapsto a^r d^s$. We define a map $\varphi(k,r) : \mathrm{Pol}_k(r) \to \mathrm{ind}_{\mathrm{B}}^{\mathrm{GL}_2(\mathbf{F}_p)} \chi(r, r+k)$ as follows: the image of a polynomial P is the function on $\mathrm{GL}_2(\mathbf{F}_p)$ that sends g to $(\rho_{\mathrm{Pol}_k(r)}(g)P)(0,1)$.

Exercise 26. *Check that $\varphi(k,r)$ is an intertwining operator $\mathrm{Pol}_k(r) \to \mathrm{ind}_{\mathrm{B}}^{\mathrm{GL}_2(\mathbf{F}_p)} \chi(r, r+k)$.*

The image of $\varphi(k,r)$ is therefore a subrepresentation of $\mathrm{ind}_{\mathrm{B}}^{\mathrm{GL}_2(\mathbf{F}_p)} \chi(r, r+k)$.

Exercise 27. *Show that if $0 \leq k \leq p-1$, $\mathrm{ind}_{\mathrm{B}}^{\mathrm{GL}_2(\mathbf{F}_p)} \chi(r, r+k)$ contains a subrepresentation isomorphic to $\mathrm{Pol}_k(r)$.*

Exercise 28. *Show that if $0 \leq k \leq p-1$, $\mathrm{ind}_{\mathrm{B}}^{\mathrm{GL}_2(\mathbf{F}_p)} \chi(r, r+k)$ has a quotient representation isomorphic to $\mathrm{Pol}_{p-1-k}(r+k)$.*

Hint: use the contragredient.

Exercise 29. *Show that if $0 \leq k \leq p-1$, then*

$$\mathrm{Irr}(\mathrm{ind}_{\mathrm{B}}^{\mathrm{GL}_2(\mathbf{F}_p)} \chi(r, r+k)) = \{\mathrm{Pol}_k(r), \mathrm{Pol}_{p-1-k}(r+k)\}.$$

7. End of the proof of Theorem 1

Let V be a representation of $\mathrm{GL}_2(\mathbf{F}_p)$. We denote by $V|_{\mathrm{B}}$ the restriction of this representation to B: it is the representation given by the restriction to B of the morphism $\mathrm{GL}_2(\mathbf{F}_p) \to \mathrm{Aut}(V)$.

Exercise 30. *Let V be a finite dimensional $\mathbf{F}_p$-representation of $\mathrm{GL}_2(\mathbf{F}_p)$. Show that there exists a multiplicative map $\chi : \mathrm{B} \to \mathbf{F}_p^\times$ such that $V|_{\mathrm{B}}$ contains a subrepresentation isomorphic to χ.*

Hint: consider V^{U}.

Exercise 31. *Let V be a finite dimensional $\mathbf{F}_p$-representation of $\mathrm{GL}_2(\mathbf{F}_p)$.*

1. *Show that V has a subrepresentation isomorphic to $\mathrm{Pol}_k(r)$ for some r and some $0 \leq k \leq p-1$. Hint: use exercise 23.*
2. *Finish the proof of theorem 1.*

8. More about the representations $\mathrm{Pol}_k(r)$

Let V be a representation of a group G, and W be an irreducible representation of G. Let us denote by $[V : W]$ the number of irreducible constituents of V that are isomorphic to W; this is called the *multiplicity* of W in V.

Exercise 32. *Suppose that V has a central character. Show that $[V : W] = 0$ if the central character of W is not the same as the central character of V.*

We now return to representations of $\mathrm{GL}_2(\mathbf{F}_p)$. Our goal in this section is to understand how $[\mathrm{Pol}_k(r) : W]$ varies if W is fixed and $k \to +\infty$. Recall that $D = x^p y - xy^p$.

Exercise 33. *Show that "multiplication by D" defines a morphism of representations $\mathrm{Pol}_k(r+1) \to \mathrm{Pol}_{k+p+1}(r)$, so that $\mathrm{Pol}_{k+p+1}(r)$ has a subrepresentation isomorphic to $\mathrm{Pol}_k(r+1)$.*

We now extend a little the result of exercise 27.

Exercise 34. *Suppose that $k \geq p+1$. Show that there exists a morphism of representations $\mathrm{Pol}_k(r) \to \mathrm{ind}_{\mathrm{B}}^{\mathrm{GL}_2(\mathbf{F}_p)} \chi(r, r+k)$ whose kernel is the image of $\mathrm{Pol}_{k-p-1}(r+1)$ by multiplication by D, and which is surjective.*

Exercise 35. *Give a recursive formula expressing $[\mathrm{Pol}_k(r) : \mathrm{Pol}_a(b)]$ in terms of $[\mathrm{Pol}_{k-p-1}(r+1) : \mathrm{Pol}_a(b)]$ and $[\mathrm{ind}_{\mathrm{B}}^{\mathrm{GL}_2(\mathbf{F}_p)} \chi(r, r+k) : \mathrm{Pol}_a(b)]$ for an irreducible representation $\mathrm{Pol}_a(b)$.*

Exercise 36. *Fix $0 \leq a \leq p-1$ and $0 \leq b \leq p-2$ and $0 \leq r \leq p-2$. Set $\delta = 1$ if $a = 0$ or $a = p-1$, and $\delta = 2$ otherwise.*

Show that $[\mathrm{Pol}_k(r) : \mathrm{Pol}_a(b)] = 0$ if $p-1$ does not divide $(k+2r) - (a+2b)$, and that

$$\frac{[\mathrm{Pol}_k(r) : \mathrm{Pol}_a(b)]}{\dim \mathrm{Pol}_k(r)} \to \frac{\delta}{p^2-1},$$

as $k \to +\infty$ with the condition that $p-1$ divides $(k+2r) - (a+2b)$.

9. Generalization to $\mathrm{GL}_2(\mathbf{F}_q)$

We fix an algebraic closure $\overline{\mathbf{F}}_p$ of $\mathbf{F}_p$. The map $\varphi : x \mapsto x^p$ is an automorphism of $\overline{\mathbf{F}}_p$. If $q = p^d$ with $d \geq 1$, then let $\mathbf{F}_q = \{x \in \overline{\mathbf{F}}_p \text{ such that } \varphi^d(x) = x\}$.

Exercise 37. *Show that $\mathbf{F}_q$ is a field with q elements, and that any extension of $\mathbf{F}_p$ of degree d (inside $\overline{\mathbf{F}}_p$) is equal to $\mathbf{F}_q$.*

Exercise 38. *Prove that there exists $g \in \mathbf{F}_q^\times$ such that $\mathbf{F}_q^\times = \{1, g, \ldots, g^{q-2}\}$ (more generally, you could prove that if F is any field and W is a finite subgroup of $F^\times$, then W is cyclic).*

Show that every multiplicative map $f : \mathbf{F}_q^\times \to \mathbf{F}_q^\times$ is of the form $x \mapsto x^r$ with $0 \leq r \leq q-2$, which can also be written as $x \mapsto x^{r_0} \cdot \varphi(x)^{r_1} \cdots \varphi^{d-1}(x)^{r_{d-1}}$, with $0 \leq r_0, \ldots, r_{d-1} \leq p-1$.

From now on we take $q = p^d$ for some $d \geq 1$, and $E = \mathbf{F}_q$. The theory of representations of $\mathrm{GL}_2(\mathbf{F}_q)$ over E is similar to the theory of representations of $\mathrm{GL}_2(\mathbf{F}_p)$ but with some new features.

Recall that $\varphi : x \mapsto x^p$ is an automorphism of $\mathbf{F}_q$, which is of order exactly d. For $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{F}_q)$, we set $\varphi(g) = \left(\begin{smallmatrix} \varphi(a) & \varphi(b) \\ \varphi(c) & \varphi(d) \end{smallmatrix}\right)$. Let V be a representation of $\mathrm{GL}_2(\mathbf{F}_q)$ with coefficients in E. We denote by $V^{[1]}$ the representation with the same underlying vector space, and $\rho_{V^{[1]}}(g) = \rho_V(\varphi(g))$. More generally we define $V^{[n]}$ by $\rho_{V^{[n]}}(g) = \rho_V(\varphi^n(g))$, so that $V^{[n]}$ is the same as V, but with a "twisted" action of $\mathrm{GL}_2(\mathbf{F}_q)$.

Exercise 39. *Suppose that V has a central character. Give the central character of $V^{[i]}$ in terms of the central character of V.*

We still denote by $\mathrm{Pol}_k(r)$ the representation of $\mathrm{GL}_2(\mathbf{F}_q)$ on the set of homogenous polynomials of degree k with coefficients in $E = \mathbf{F}_q$.

In exercise 40 below, you need the *tensor product* of two representations of G. Here is a quick definition: if V and W are two E-vector spaces, with bases $v_1, \ldots, v_m$ and $w_1, \ldots, w_n$, then the tensor product $V \otimes W$ is the E-vector space with basis the mn elements $v_i \otimes w_j$. If $f \in \mathrm{End}(V)$ and $g \in \mathrm{End}(W)$ are given by $f(v_i) = \sum_k f_{ik} v_k$ and $g(w_j) = \sum_\ell g_{j\ell} w_\ell$, then $f \otimes g \in \mathrm{End}(V \otimes W)$ is given by $(f \otimes g)(v_i \otimes w_j) = \sum_{k,\ell} f_{ik} g_{j\ell} \cdot v_k \otimes w_\ell$. If V and W are representations of G, then we make $V \otimes W$ into a representation of G by setting $\rho_{V \otimes W}(g) = \rho_V(g) \otimes \rho_W(g)$. You should look up the definition of the tensor product in different textbooks and compare it with the one given here.

Exercise 40. *Show that Pol_{kp} contains a subrepresentation isomorphic to $\mathrm{Pol}_k^{[1]}$.*

Write $k = \sum_{i=0}^m k_i p^i$ with $0 \leq k_i \leq p-1$. Show that Pol_k contains a subrepresentation isomorphic to $\mathrm{Pol}_{k_0}^{[0]} \otimes \mathrm{Pol}_{k_1}^{[1]} \otimes \cdots \otimes \mathrm{Pol}_{k_m}^{[m]}$.

The analogue of theorem 1 is the following.

Theorem 2. *The set of irreducible representations of $\mathrm{GL}_2(\mathbf{F}_q)$ with coefficients in E is exactly the set of representations of the form $(\otimes_{i=0}^{d-1} \mathrm{Pol}_{a_i}^{[i]})(b)$ for $0 \leq a_i \leq p-1$ and $0 \leq b \leq q-2$, and these representations are pairwise non isomorphic.*

You should try to prove this theorem using similar methods to those we used for $\mathrm{GL}_2(\mathbf{F}_p)$. Can you do the analogue of exercise 36 for $\mathrm{GL}_2(\mathbf{F}_q)$? This is theorem 3.1 of [Roz14].

10. Suggestions for further study

If you're done proving theorem 2, you can try to see what happens for $\mathrm{GL}_n(\mathbf{F}_q)$ if $n \geq 3$. What are the analogues for GL_n of the representations Pol_k? Of the parabolic inductions?

The article [Glo78] contains a number of properties of the representations Pol_k of GL_2 (his V_m is our Pol_{m-1}). Can you understand what are the main results of [Glo78]?

Another possibility is to study E-linear representations of $\mathrm{GL}_2(\mathbf{F}_q)$ if E is a field of characteristic $\neq p$, for example the complex numbers. This was first done by Jordan and Schur in 1907 (see [Jor07] and [Sch07], and [FH91] or [AB95] for a more modern approach). The representations Pol_k don't exist anymore, but the $\mathrm{ind}_{\mathrm{B}}^{\mathrm{GL}_2(\mathbf{F}_p)}\chi$ still do. How much of the proof can you salvage? At some point, you'll have to consider irreducible representations V such that $V^{\mathrm{U}} = \{0\}$. These are called *cuspidal* representations.

Finally, the motivation for our own interest in these representations of $\mathrm{GL}_2(\mathbf{F}_p)$ is that they are the starting point for constructing $\mathbf{F}_p$-representations of $\mathrm{GL}_2(\mathbf{Z}_p)$ and $\mathrm{GL}_2(\mathbf{Q}_p)$, where $\mathbf{Z}_p$ are the p-adic integers and $\mathbf{Q}_p$ is the field of p-adic numbers. These representations play a very important role in the *p-adic local Langlands correspondence*.

References

[AB95] Jonathan Lazare Alperin and Rowen B. Bell, *Groups and representations*, Graduate Texts in Mathematics, vol. 162, Springer-Verlag, New York, 1995.

[BN41] Richard Dagobert Brauer and Cecil Nesbitt, *On the modular characters of groups*, Ann. of Math. (2) **42** (1941), 556–590.

[CR06] Charles Whittlesey Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, AMS Chelsea Publishing, Providence, RI, 2006, Reprint of the 1962 original.

[FH91] William Fulton and Joe Harris, *Representation theory*, Graduate Texts in Mathematics, vol. 129, Springer-Verlag, New York, 1991, A first course, Readings in Mathematics.

[Glo78] David John Glover, *A study of certain modular representations*, J. Algebra **51** (1978), no. 2, 425–475.

[Jor07] Herbert Edwin Jordan, *Group-Characters of Various Types of Linear Groups*, Amer. J. Math. **29** (1907), no. 4, 387–405.

[Lan02] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[Roz14] Sandra Rozensztajn, *Asymptotic values of modular multiplicities for* GL_2, J. Théor. Nombres Bordeaux **26** (2014), no. 2, 465–482.

[Sch07] Issai Schur, *Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen.*, J. Reine Angew. Math. **132** (1907), 85–137.

Laurent Berger, ENS de Lyon, Lyon, France
E-mail address: laurent.berger@ens-lyon.fr
URL: perso.ens-lyon.fr/laurent.berger/

Sandra Rozensztajn, ENS de Lyon, Lyon, France
E-mail address: sandra.rozensztajn@ens-lyon.fr
URL: perso.ens-lyon.fr/sandra.rozensztajn/