

Problem Sheet 1 - EXTRA BONUS PROBLEM

Let p be a prime number, and let $k = \mathbb{F}_p$ the field with p elements. So $\mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$.

Note that since the field k has p elements, the vector space k^2 has p^2 elements, k^3 has p^3 elements, and so forth.

Recall in class we considered the n -dimensional *projective space* over k , $X = k\mathbb{P}^n$, as the set of 1-dimensional linear subspaces ℓ of k^{n+1} , and showed that it has $\frac{p^{n+1}-1}{p-1}$ many elements. So:

$$|k\mathbb{P}^n| = \frac{p^{n+1} - 1}{p - 1} = 1 + p + \cdots + p^n, \quad \text{if } k = \mathbb{F}_p.$$

Namely, we realized that the points in X can be identified with orbits of the multiplicative group k^\times of k acting by scalar multiplication on the set $k^{n+1} \setminus \{0\}$. And then we counted how many such orbits there were using the Cauchy-Frobenius formula.

Note that alternatively we could have said $k^{n+1} \setminus \{0\}$ has $p^{n+1} - 1$ elements, and each spans a unique “line” ℓ in k^{n+1} . So we have found $p^{n+1} - 1$ lines in k^{n+1} . But these lines are not all distinct. Namely, since each line ℓ has $p - 1$ distinct non-zero elements, it has been counted $p - 1$ times in the $p^{n+1} - 1$ lines. Therefore there are in fact $\frac{p^{n+1}-1}{p-1}$ lines in k^{n+1} . Thus we have checked the above formula for $|k\mathbb{P}^n|$ in another way and can now be doubly certain!

PROBLEM:

(1) Suppose $n = 1$ above, so that $X = k\mathbb{P}^1$. Let $G = SL_2(k)$ act on k^2 in the usual way by k -linear transformations. Show that this also defines an action of $SL_2(k)$ on $X = k\mathbb{P}^1$.

(2) Show that the action of $SL_2(k)$ on $X = k\mathbb{P}^1$ is transitive.

(3) Describe the stabilizer subgroup G_ℓ , for the point $\ell \in X$ given by $\ell = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle$.

(4) Using (1-3) and the orbit stabilizer lemma, derive the formula for the order of the finite group $G = SL_2(\mathbb{F}_p)$:

$$|SL_2(\mathbb{F}_p)| = (p - 1)p(p + 1)$$

[Note: In parts (1), (2) and (3) the field k can be an arbitrary field. In part (4) use $k = \mathbb{F}_p$.]