

# 1 The order of $\mathrm{GL}(n, \mathbb{F}_q)$ and $\mathrm{SL}(n, \mathbb{F}_q)$ over a finite field

The other day I wanted to know the order of  $\mathrm{SL}(n, \mathbb{F}_q)$  over the field  $F$  of  $q$  elements. A number of different Google searches failed to find even an expression for the order of the group, to say nothing of a proof. So here I remedy those deficiencies of the World Wide Web.

$\mathrm{GL}(n, \mathbb{F}_q)$  is the group of  $n \times n$  invertible matrices with entries in the field of  $q$  elements (of course,  $q$  is necessarily a power of a prime, but we won't need that here).  $\mathrm{SL}(n, \mathbb{F}_q)$  is the group of  $n \times n$  invertible matrices with determinant 1. We'll deal with  $\mathrm{GL}(n, \mathbb{F}_q)$  first:

**Theorem 1.** *The order of  $\mathrm{GL}(n, \mathbb{F}_q)$  is  $(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$ .*

*Proof.* Take a matrix  $A \in \mathrm{GL}(n, \mathbb{F}_q)$ . Think of column  $i$  of the matrix as the image of the  $i$ th basis vector in  $F^n$ . For the first column, we may choose any nonzero vector in  $F^n$ , so there are  $q^n - 1$  choices for that column. For the second column, we may choose any vector that it is not in the 1-dimensional subspace spanned by the first column. There are  $q$  points in that subspace, so there are  $q^n - q$  choices. For the third column, we must avoid points in the 2-dimensional subspace (that has  $q^2$  points), and so on. The order of  $\mathrm{GL}(n, \mathbb{F}_q)$  is therefore

$$(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}). \quad \square$$

Now it is easy to find out the size of  $\mathrm{SL}(n, \mathbb{F}_q)$ : the determinant is a homomorphism from  $\mathrm{GL}(n, \mathbb{F}_q)$  to  $F^*$ , the nonzero elements of  $F$ . The kernel of this homomorphism is exactly  $\mathrm{SL}(n, \mathbb{F}_q)$ , which means (by what is often called the First Isomorphism Theorem) the quotient group is isomorphic to  $F^*$ . Now just "take orders" (find the order of each side):

$$\left| \frac{\mathrm{GL}(n, \mathbb{F}_q)}{\mathrm{SL}(n, \mathbb{F}_q)} \right| = |F^*| = q - 1 \quad \implies \quad \frac{|\mathrm{GL}(n, \mathbb{F}_q)|}{|\mathrm{SL}(n, \mathbb{F}_q)|} = q - 1,$$

since our groups are finite. Now just rearrange, and the prayers of up-late-studying-for-prelims grad students are answered:

$$|\mathrm{SL}(n, \mathbb{F}_q)| = \frac{|\mathrm{GL}(n, \mathbb{F}_q)|}{q - 1} = \frac{(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})}{q - 1}.$$

I should note that this material is basically stolen from [2], page 74. These two proofs are exercises in [1], page 546.

## 1.1 A mild generalization to non-fields

It's relatively easy to find the order of  $\mathrm{GL}(n, \mathbb{Z}/m\mathbb{Z})$  when  $m$  is a square-free prime. Say  $m = p_1 p_2 \cdots p_k$ . Then given a matrix in  $\mathrm{GL}(n, \mathbb{Z}/m\mathbb{Z})$ , there's an obvious bijection using the Chinese Remainder Theorem:

$$\begin{aligned} \text{matrices over } \mathbb{Z}/m\mathbb{Z} &\longleftrightarrow \{ \text{matrices over } \mathbb{Z}/p_1\mathbb{Z} \} \times \{ \text{matrices over } \mathbb{Z}/p_2\mathbb{Z} \} \times \cdots \\ &\quad \cdots \times \text{matrices over } \mathbb{Z}/p_k\mathbb{Z} \end{aligned}$$

The bijection works by reducing every entry in the matrix modulo  $p_i$ . This is actually a homomorphism of rings: as an additive homomorphism, it's obvious, and multiplicatively it's also easy to see. It's a bijection and a homomorphism, hence an isomorphism:

$$\mathrm{GL}(n, \mathbb{Z}/m\mathbb{Z}) \cong \bigoplus_{i=1}^k \mathrm{GL}(n, \mathbb{Z}/p_i\mathbb{Z}). \quad (1)$$

Of course, for the purpose of calculating the order we don't care about isomorphisms. The order of each summand on the right side of (1) is just as above, which means

$$|\mathrm{GL}(n, \mathbb{Z}/m\mathbb{Z})| = \prod_{i=1}^k \left( \prod_{j=0}^{m-1} (p_i^m - p_i^j) \right). \quad \square$$

## 1.2 Where to go next

What I should really add to this:

- What if  $m$  isn't square-free? Then the Chinese Remainder theorem gives you a bijection to the ring  $\mathbb{Z}/p^k\mathbb{Z}$ , not the field with  $p^k$  elements.
- SL for  $m$  not prime. Probably little change required from the first section.

## References

- [1] Serge Lang, *Algebra*, 3rd ed., Addison-Wesley, 1993.
- [2] Derek J.S. Robinson, *A course in the theory of groups*, 2nd ed., Springer-Verlag, 1996.