

## ORDER OF ELEMENTS IN $SL(2, p)$

ONDREJ ŠUCH

The purpose of this note is to look at the simple question: “What are the orders of elements of the group  $SL(2, p)$ ?” This group is treated at the graduate level for instance in [Lang]. However, we feel that a great deal about this group can be explained to college students with hardly more background than an introductory linear algebra course. We hope that our approach can explain to students why one works with the trace of a matrix, the Cayley-Hamilton theorem, or finite fields.

### 1. USING THE CAYLEY-HAMILTON THEOREM

For two-by-two matrices, it is straightforward to verify the *Cayley-Hamilton theorem*, i.e. that for any  $2 \times 2$  matrix  $\mathbf{A}$  one has

$$\mathbf{A}^2 - \text{tr}(\mathbf{A}) \cdot \mathbf{A} + \det(\mathbf{A}) \cdot \mathbf{I} = \mathbf{0} \quad (1.1)$$

with the usual definitions  $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$  and  $\text{tr}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a + d$ .

**1.1. Involutions.** To illustrate usefulness of this theorem, let us start by finding *involutions* in groups  $SL(2, p)$ , where  $p$  is a prime. If  $\mathbf{A}$  is a matrix satisfying  $\mathbf{A}^2 = \mathbf{I}$  then from (1.1) we have

$$2\mathbf{I} = \text{tr}(\mathbf{A}) \cdot \mathbf{A}$$

If  $p \neq 2$ , then  $\mathbf{A}$  has to be a scalar multiple of identity, say  $\lambda \cdot \mathbf{I}$ , with

$$2\lambda^2 \equiv 2 \pmod{p}$$

It follows that  $-\mathbf{I}$  is the only involution in the group  $SL(2, p)$  for odd  $p$ . If on the other hand  $p = 2$  we get  $\mathbf{0} = \text{tr}(\mathbf{A}) \cdot \mathbf{A}$  which implies that  $\text{tr}(\mathbf{A})$  has to be zero. If  $\mathbf{A}$  is not the identity, the converse holds as well. Namely, it follows from (1.1) that  $\mathbf{A}^2 = \mathbf{I}$ . Thus the involutions in  $SL(2, 2)$  are the matrices

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

**1.2. Orders of elements in the group  $SL(2, 3)$ .** We can put Cayley-Hamilton theorem to further use. Any element  $\mathbf{A}$  of  $SL(2, 3)$  satisfies one of the three equations

$$\mathbf{A}^2 - \mathbf{A} + \mathbf{I} = \mathbf{0} \quad (1.2)$$

$$\mathbf{A}^2 + \mathbf{I} = \mathbf{0} \quad (1.3)$$

$$\mathbf{A}^2 + \mathbf{A} + \mathbf{I} = \mathbf{0} \quad (1.4)$$

We can multiply these equations by  $\mathbf{A} + \mathbf{I}$ ,  $\mathbf{A}^2 - \mathbf{I}$  and  $\mathbf{A} - \mathbf{I}$  respectively to arrive at the equations

$$\mathbf{A}^3 = -\mathbf{I}$$

$$\mathbf{A}^4 = \mathbf{I}$$

$$\mathbf{A}^3 = \mathbf{I}$$

From these equations it follows that

---

*Key words and phrases.* Linear groups.

- any element with trace 1, other than  $-\mathbf{I}$ , is of order 6,
- any element with trace 0 is of order 4,
- any element with trace -1, other than  $\mathbf{I}$ , is of order 3.

Let us make a small detour. Visualizations are very important when teaching students. There is a little known visualization of  $SL(2,3)$  due to V. Proulx [Prou]. The picture shown in Figure 1 is called the *Cayley graph* for the group  $G := \langle x, y \mid x^3 = y^3 = 1, xyx = yxy \rangle$ .

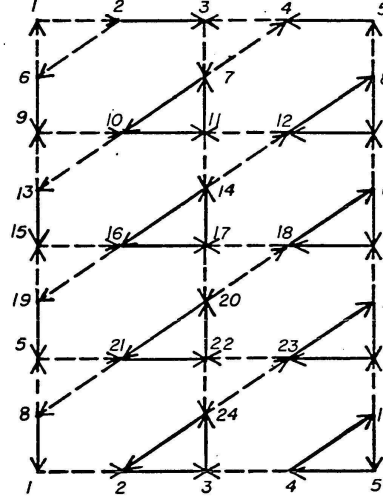


FIGURE 1. Cayley graph of  $SL(2,3)$

The group  $G$  acts on vertices of the graph as follows: the generator  $x$  moves a vertex along a solid line, and the generator  $y$  moves a vertex along a dashed line in the direction of the arrow. When the boundary of the rectangle is folded by identifying opposite sides of the rectangle so that vertices with same numbers coincide, one obtains embedding of the graph on the torus.

It is quite easy to read off relations between generators from a Cayley graph. Any closed walk corresponds to a relation. It is less clear, that the graph actually represents group  $SL(2,3)$ . Students can however use the knowledge of which elements of  $SL(2,3)$  have order 3 to find an isomorphism between  $G$  and  $SL(2,3)$ . One such isomorphism is given by:

$$x \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 0 & 1 \\ 2 & 2 \end{pmatrix}$$

**1.3. Orders of elements in  $SL(2,5)$ .** Over the field with 5 elements there are two more equations elements of  $SL(2,5)$  can satisfy besides (1.2)-(1.4):

$$\mathbf{A}^2 - 2\mathbf{A} + \mathbf{I} = 0 \tag{1.5}$$

$$\mathbf{A}^2 + 2\mathbf{A} + \mathbf{I} = 0 \tag{1.6}$$

In the first case set  $\mathbf{M} := \mathbf{A} - \mathbf{I}$ . Then equation (1.5) implies  $\mathbf{M}^2 = \mathbf{0}$  i.e. that the matrix  $\mathbf{M}$  is *nilpotent*. Moreover,  $\mathbf{M}$  commutes with  $\mathbf{A}$  (as does any polynomial expression in  $\mathbf{A}$ ). Thus we have a binomial expansion

$$\begin{aligned} \mathbf{A}^n &= \mathbf{I}^n + \binom{n}{1} \mathbf{I}^{n-1} \mathbf{M} + \binom{n}{2} \mathbf{I}^{n-2} \mathbf{M}^2 + \dots \\ &= \mathbf{I} + n\mathbf{M}. \end{aligned}$$

In particular we get  $\mathbf{A}^5 = \mathbf{I}$ . Thus if  $\text{tr}(\mathbf{A}) = 2$  and  $\mathbf{A} \neq \mathbf{I}$  then the order of  $\mathbf{A}$  is 5.

Similarly, if  $\mathbf{A}$  satisfies (1.6), one sets  $\mathbf{N} := \mathbf{I} + \mathbf{A}$  and gets that  $\mathbf{N}^2 = \mathbf{0}$  and commutes with  $\mathbf{A}$ . Thus

$$\begin{aligned} \mathbf{A}^n &= (\mathbf{N} - \mathbf{I})^n = \mathbf{N}^n - \binom{n}{1} \mathbf{N}^{n-1} \mathbf{I} + \dots + (-1)^{n-1} \binom{n}{n-1} \mathbf{N} \mathbf{I}^{n-1} + (-1)^n \mathbf{I}^n \\ &= (-1)^n (\mathbf{I} - n\mathbf{N}) \end{aligned}$$

It follows that if  $\text{tr}(\mathbf{A}) = -2$  and  $\mathbf{A} \neq -\mathbf{I}$  then the order of  $\mathbf{A}$  is 10.

**1.4. Orders of elements in  $SL(2, 7)$ .** In this group there are elements with trace  $\pm 3$ . It would seem we have run out of tricks with Cayley-Hamilton theorem, but that is not the case. Taking the trace of the matrices in (1.1) we obtain

$$\text{tr}(\mathbf{A}^2) - \text{tr}(\mathbf{A})\text{tr}(\mathbf{A}) + \text{tr}(\mathbf{I}) = 0, \quad (1.7)$$

thus if  $\text{tr}(\mathbf{A}) = \pm 3$  we have

$$\text{tr}(\mathbf{A}^2) = 0.$$

In particular  $\mathbf{A}^2$  is of order 4, thus  $\mathbf{A}$  has to be of order 8.

## 2. USING FACTORIZATION OF THE CHARACTERISTIC POLYNOMIAL

For groups  $SL(2, 3)$ ,  $SL(2, 5)$ ,  $SL(2, 7)$  clever application of Cayley-Hamilton theorem quickly yielded order of its elements based on their traces. This allowed us to circumvent the underlying computation that determines the order of an element  $\mathbf{A}$ , namely determining the lowest  $n$  such that the characteristic polynomial divides  $X^n - 1$ .

To continue further, we will consider how the characteristic polynomial  $\chi(x)$  of the matrix  $\mathbf{A}$  factors modulo  $p$ . In principle there are three possibilities

- it is a perfect square of a linear term
- it factors as the product of two distinct linear terms
- it is irreducible

**2.1. Characteristic polynomial is a perfect square.** The structure of a complex matrix with multiple roots of characteristic polynomial is usually characterized by the Jordan decomposition theorem. Fortunately, in our case we will not need to invoke such a theorem. First, since  $\det(\mathbf{A}) = 1$ , it follows that  $\chi(x)$  is either  $(x-1)^2$  or  $(x+1)^2$ . We have considered this problem in 1.3 and have the following result:

**Proposition 1.** *Let  $p$  be an odd number and  $\mathbf{A}$  a matrix in  $SL(2, p)$  whose characteristic polynomial is a square. Then  $\text{tr}(\mathbf{A}) = \pm 2$ .*

- a) *If the trace of the matrix  $\mathbf{A}$  is 2, then either  $\mathbf{A}$  is the identity, or the order of  $\mathbf{A}$  is  $p$ .*
- b) *If the trace of the matrix  $\mathbf{A}$  is  $-2$ , then either  $\mathbf{A} = -\mathbf{I}$  or the order of  $\mathbf{A}$  is  $2p$ .*

**2.2. Characteristic polynomial is the product of distinct linear terms.** Say  $\chi(x) = (x - \lambda_1)(x - \lambda_2)$ . Then matrices  $\mathbf{A} - \lambda_1 \cdot \mathbf{I}$  and  $\mathbf{A} - \lambda_2 \cdot \mathbf{I}$  are singular, thus there are non-zero vectors  $\mathbf{v}_1, \mathbf{v}_2$  in their corresponding null spaces. If  $\mathbf{P}$  is the matrix with vectors  $\mathbf{v}_1, \mathbf{v}_2$  as its columns, we have

$$\mathbf{A} = \mathbf{P} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \mathbf{P}^{-1}$$

and for any  $n \geq 1$

$$\mathbf{A}^n = \mathbf{P} \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix} \mathbf{P}^{-1} \quad (2.1)$$

We obtain the following result

**Proposition 2.** *The order of  $\mathbf{A}$  is equal to the order of  $\lambda_1$  in the multiplicative group  $\mathbf{F}_p^\times$ .*

*Proof.* First we remark that the orders of  $\lambda_1$  and  $\lambda_2 = 1/\lambda_1$  are necessarily equal. If  $\lambda_1^n = 1$  then from (2.1) it follows that  $\mathbf{A}^n = 1$ . Conversely, if  $\mathbf{A}^n = 1$ , then  $\mathbf{A}^n \mathbf{v}_1 = \mathbf{v}_1$  but then from (2.1) we get  $\lambda_1^n = \lambda_2^n = 1$ .  $\square$

**2.3. Irreducible characteristic polynomial.** This situation arises for instance when  $p = 11$  and  $\text{tr}(\mathbf{A}) = 5$ . Then the polynomial  $x^2 - 5x + 1$  is irreducible. We can try to mimic the approach used to solve irreducible polynomials over real numbers. Let us consider the set  $\mathbf{F}$  of sums  $a + bI$ , where  $I^2 = -1$ . The crucial property of complex numbers, namely division, carries over to this set. Indeed the existence of division by nonzero numbers relies upon the identity

$$\frac{1}{a + bI} = \frac{1}{a + bI} \cdot \frac{a - bI}{a - bI} = \frac{a - bI}{a^2 + b^2}.$$

We can do the same for  $p = 11$  as well, since  $a^2 + b^2$  is never 0 modulo 11 for a pair of integers  $a, b$  at least one of which is not divisible by 11!

Returning to  $\mathbf{A}$  we can carry out reasoning analogously to Proposition 2 that the order of  $\mathbf{A}$  is equal to the order of a root of  $x^2 - 5x + 1$  in  $\mathbf{F}^\times$ . Substituting  $x = a + bI$  into  $\chi(x)$  we obtain  $a = 8$  and  $b = \pm 5$ . We have

$$(8 + 5I)^2 = 6 + 3I, \quad (8 + 5I)^3 = -1$$

from where it follows that the order of  $\mathbf{A}$  is 6.

Actually, in this case we could avoid our detour to the set  $\mathbf{F}$  by an alternate argument. Since  $\text{tr}(\mathbf{A}) = 5$  we have from (1.7) that  $\text{tr}(\mathbf{A}^2) = 1$ . It follows that the order of  $\mathbf{A}^2$  is 3. Thus the order of  $\mathbf{A}$  can be either 3 or 6, but it cannot be 3, for then  $\mathbf{A} = \mathbf{A}^4$  and we have again by (1.7) that  $\text{tr}(\mathbf{A}^4) = -1 \neq 5 = \text{tr}(\mathbf{A})$ .

Both approaches just described fail when  $p = 13$ . Let us see why the latter approach fails. The order of group  $\text{SL}(2, 13)$  is  $13(13^2 - 1) = 2^3 \cdot 3 \cdot 7 \cdot 13$ . By Lagrange's theorem there is an element  $g$  of order 7 in  $G$ . If we square it, we obtain elements  $g, g^2, g^4$  and nothing else, all of them of order 7. However, no element of  $\mathbf{F}_{13}^\times$  has order 7, since the group has order 12. The former approach fails because  $13 = 2^2 + 3^2$  thus adjoining  $I$  to  $\mathbf{F}_{13}$  does not yield a set in which we can divide.

The former approach can be repaired however, and in fact for any odd prime  $p$ . The key is to notice that the map  $x \rightarrow x^2$  from  $\mathbf{F}_p^\times$  to  $\mathbf{F}_p^\times$  is not bijective, since 1 and -1 are both mapped to one<sup>1</sup>. Thus there is an  $\alpha$  such that equation  $x^2 = \alpha$  has no solution in  $\mathbf{F}_p$ . We can then consider the set  $\mathbf{F}_p[\beta]$  of linear combinations  $a + b\beta$ , on which we define multiplication by  $\beta^2 = \alpha$ . The question whether we can divide is answered by the following computation:

$$\frac{1}{a + b\beta} = \frac{1}{a + b\beta} \cdot \frac{a - b\beta}{a - b\beta} = \frac{a - b\beta}{a^2 - b^2\alpha},$$

and the denominator of the last expression cannot be 0, because then we would have  $\left(\frac{a}{b}\right)^2 = \alpha$ , contrary to our choice of  $\alpha$ . Computing explicitly we obtain the following result.

<sup>1</sup>Note also that the range of the map excludes  $-1$  for  $p = 11$  which is why adjoining  $I$  worked in that case, and includes  $-1$  for  $p = 13$ , which is why adjoining  $I$  did not work then.

**Proposition 3.** *Let  $\mathbf{A}$  be an element of  $SL(2, p)$  where  $p > 2$  such that its characteristic polynomial  $x^2 - tx + 1$  is irreducible over  $\mathbf{F}_p$ . Let  $\alpha$  be a nonsquare in  $\mathbf{F}_p^\times$ . Then the order of  $\mathbf{A}$  in  $SL(2, p)$  is equal to the order of  $\frac{t}{2} + \beta\sqrt{\frac{t^2-4}{4\alpha}}$  in the multiplicative group of the field  $\mathbf{F}_p[\beta]$ .*

A nice corollary of this result is that an order of element with irreducible characteristic polynomial divides  $p^2 - 1$ . Indeed, the size of the multiplicative group  $\mathbf{F}[\beta]^\times$  is  $p^2 - 1$  and the order of an element divides the order of the group.

### 3. CONCLUSION

We have shown that knowing little more than the trace of an element in the group  $SL(2, p)$  we can determine its order. We can only concur to [Mac1] and [Mac2] that linear groups over finite examples are quite suitable as examples in teaching of college algebra.

Perhaps the only less than satisfactory feature of the group  $SL(2, p)$  is the lack of visualization for  $p > 3$ . It would be very interesting to find visualizations of  $SL(2, p)$  for higher  $p$ , such as the visualization of  $SL(2, 3)$  presented in the text.

### REFERENCES

- [Lang] Lang, S., *Algebra*, 3rd edition, Addison-Wesley 1993
- [Mac1] Mackiw, G. Computing in Abstract Algebra, *The College Mathematics Journal*, Vols. 27, No.2 (Mar., 1996), pp. 136-142
- [Mac2] Mackiw, G. The Linear Group  $SL(2, 3)$  as a source of Examples *The Mathematical Gazette*, Vol. 81, No. 490 (Mar. 1997), pp. 64-67
- [Prou] Proulx, V., Classification of the Toroidal Groups, Ph.D. thesis, Columbia University, 1977

UNIVERSITY OF MATEJ BEL, TAJOVSKÉHO 40, 974 01 BANSKÁ BYSTRICA, SLOVAK REPUBLIC,  
E-mail address: such@fpv.umb.sk