Simple Groups

Definition. A group is *simple* if it has no proper non-trivial normal subgroup.

Camille Jordan
1838 — 1922
known for
- Jordan curve
- Jordan-Hölder theorem
- canonical Jordan form
- Jordan algebra

The simplicity of A_n for $n \geq 5$.

Lemma 7.1

1) For $n \geq 3$, A_n is generated by permutations (abc)

2) For $n \geq 5$, A_n is generated by permutations of type $(ab)(cd)$, with a,b,c,d distinct.

Proof.

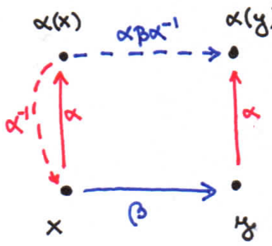
1) $(ac)(ab) = (abc)$

$(ac)(bd) = (ac)\underbrace{(ab)(ab)}_{\text{identity}}(bd) = (abc)(abd)$

Therefore, if we have at least 3 letters, a permutation which is a product of even number of transpositions is a product of 3-cycles.

2) $(abc) = (ac)(de)(de)(bc)$ – here, since we have at least 5 letters, we can add d, e distinct then a, b, c. □

⚠ Let α, β be permutations. If $\beta(x) = y$, then $(\alpha\beta\alpha^{-1})(\alpha(x)) = \alpha(y)$:



Lemma 7.2. The decomposition of the permutation $\alpha\beta\alpha^{-1}$ into disjoint cycles can be obtained from the analogous decomposition of β by replacing x by $\alpha(x)$.

Proof. We apply the previous observation:

$$\beta = (\ldots)(\ \ldots\ )\ldots(\ldots, x, y, \ldots)\ldots(\ldots)$$

— the decomposition of β as a product of independent cycles

$$\alpha\beta\alpha^{-1} = (\ldots)(\ \ldots\ )\ldots(\ldots, \alpha(x), \alpha(y), \ldots)\ldots(\ldots)$$

— the decomposition of $\alpha\beta\alpha^{-1}$.

□

Corollary 4.3: The number of disjoint cycles of each length in the decompositions of β and $\alpha\beta\alpha^{-1}$ is the same.

Theorem 4.4: Let $n \geq 5$. Then

① A_n is the unique proper non-trivial normal subgroup of S_n.

② A_n is simple.

Proof:

① Suppose that $1 \underset{\neq}{\triangleleft} N \underset{\neq}{\triangleleft} S_n$. Let $1 \neq \sigma \in N$. Then is a such that $\sigma^{-1}(a) \neq a$. Choose $b \notin \{a, \sigma^{-1}(a)\}$. Put $\alpha = (ab)$ and $\beta = \sigma\alpha\sigma^{-1}\alpha^{-1}$. Since N is a normal subgroup of S_n, both σ and $\alpha\sigma^{-1}\alpha^{-1}$ belong to N. Therefore $\beta \in N$. On the other hand $\beta = (\sigma\alpha\sigma^{-1})\alpha^{-1}$ is a product of two transpositions. So β is of the form $(a\,b)(b\,c)$ or $(a\,b)(c\,d)$ or it is an identity. But $\beta(b) = \sigma\alpha\sigma^{-1}\alpha^{-1}(b) = \sigma\alpha\sigma^{-1}(a) = \sigma\sigma^{-1}(a) = a$. Therefore, since $a \neq b$, β is not identity. Since N is normal, it contains either all 3-cycles or all permutations of the form $(ab)(cd)$. It follows that $A_n = N$.

To prove ② we would need a Lemma:

Lemma 4.5: Let H be a minimal non-trivial normal subgroup of a group G. Then $H \cong U_1 \times \ldots \times U_k$, where U_i are isomorphic simple groups.

Proof: By induction on $|G|$. If G is simple, then $G = H$ and we can put $U_1 = G$, ~~$\cong U_1 = G$~~ – the result is trivial. Otherwise $|H| < |G|$. Let V be a non-trivial normal subgroup of the group H. (Note that V might not be a normal subgroup of G). By the inductive hypothesis, $H \cong U_1' \times \ldots \times U_\ell'$, where U_i' are isomorphic to U_j' for $i \neq j$, and the groups U_i' are simple. We prove that H is isomorphic to a product of groups isomorphic to V. Then H is a product of simple groups all isomorphic to U_i'.

- Proof that H is isomorphic to a product of simple groups isomorphic to V:

For $g \in G$: $gVg^{-1} \trianglelefteq gHg^{-1} = H$. The group $\langle gVg^{-1} \mid g \in G \rangle$, generated by all the gVg^{-1}, is normal in G and lies in H. Therefore it coincides with H. Let X be a minimal subset of G s.t. $H = \langle xVx^{-1} \mid x \in X \rangle$. For $x_0 \in X$, $x_0Vx_0^{-1} \cap \langle xVx^{-1} \mid x \in X \setminus \{x_0\} \rangle \trianglelefteq H$ (it is an intersection of two normal subgroups of H, and $x_0Vx_0^{-1} \cap \langle xVx^{-1} \mid x \in X \setminus \{x_0\} \rangle < x_0Vx_0^{-1}$

Otherwise $H = \langle xVx^{-1} \mid x \in X \setminus \{x_0\} \rangle$ which would contradict the minimality of X.
Since V and so $x_0Vx_0^{-1}$ are minimal nontrivial normal subgroups of H,
$x_0Vx_0^{-1} \cap \langle xVx^{-1} \mid x \in X \setminus \{x_0\} \rangle = 1$. Hence $H = \prod_{x \in X} xVx^{-1}$. □

(2) As A_n is a minimal normal subgroup of S_n, $A_n = U_1 \times \dots \times U_k$, where U_i's are all isomorphic to a simple group U. Then $\frac{n!}{2} = |U|^k$. By Chebyschev theorem, there is a prime between $\lfloor \frac{n}{2} \rfloor$ and n. It follows that $k = 1$ and so A_n is simple.

Proof without Chebyshev's theorem: Since $n \geq 5$; and $|A_n| = \frac{n!}{2} = |U|^k$, $2 \mid |U|$. By the Cauchy's theorem, U_1 contains an element of order 2. Such an element β is a product $\beta = \alpha_1 \cdots \alpha_m$ of disjoint transpositions. Then $\beta = \alpha_1 \beta \alpha_1^{-1}$ and so $\beta \in U_1 \cap \alpha_1 U_1 \alpha_1^{-1}$. The groups U_1 and $\alpha_1 U_1 \alpha_1^{-1}$ are simple and normal in $A_n = \alpha_1 A_n \alpha_1^{-1}$. Therefore $U_1 = \alpha_1 U_1 \alpha_1^{-1}$. Then $U_1 \trianglelefteq \langle A_n, \alpha_1 \rangle = S_n$. Therefore $U_1 = A_n$ and so A_n is simple. □

Remark: If G is a noncyclic group of order ≤ 60, then G is not simple.

Proof: A non-cyclic simple group cannot be solvable. Therefore it is not a p-group. By Burnside's theorem (Corollary of the theorem of P. Hall), it is not a group of order $p^m q^n$ for two different primes p, q. Therefore the order of possibly simple non-cyclic group of order < 60 is either $2.3.5 = 30$ or $2.3.7 = 42$.

- The number of Sylow 7-subgroups of a group of order 42 is congruent to 1 mod 7 and divides 42. It follows that there is a unique Sylow 7-subgroup. It must be normal and so the group is not simple.
- Let G be a group of order 30. Represent G as a subgroup of S_{30} via left multiplication on itself (just doing the regular Cayley representation). An element of order 2, which exists in G by the Cauchy's theorem, is then a product of 15 independent transposition (since it has no a fixed point). Therefore it is an odd permutation. The restriction of $S_{30} \to \mathbb{Z}_2$ / S_2, mapping each permutation to its sign, to G is onto. It follows that G has a subgroup of index 2. This subgroup is normal in G.

□

Recall that for a field $\mathbb{F}$:

- $GL_n(\mathbb{F})$:= the group of all regular $n \times n$ matrices with n-ties from $\mathbb{F}$
- $SL_n(\mathbb{F})$:= $\{A \in GL_n(\mathbb{F}) \mid \det A = 1\}$

$GL_n(\mathbb{F})$ is called a general linear group while $SL_n(\mathbb{F})$ a special linear group.

Definition: Let $\mathbb{F}$ be a field. We define:

- $PGL_n(\mathbb{F}) := GL_n(\mathbb{F}) / Z(GL_n(\mathbb{F}))$.
- $PSL_n(\mathbb{F}) := SL_n(\mathbb{F}) / Z(SL_n(\mathbb{F}))$.

$PGL_n(\mathbb{F})$ is called a projective linear group while $PSL_n(\mathbb{F})$ a projective special linear group.

- For a finite field $\mathbb{F}$ of size q we might use the notation $PGL_n(q)$ and $PSL_n(q)$ for $PGL_n(\mathbb{F})$ and $PSL_n(\mathbb{F})$ respectively.

(1) We have computed that $|GL_n(q)| = \prod_{i=0}^{n-1}(q^n - q^i)$. From this we infer that

- $|SL_n(q)| = \dfrac{\prod_{i=0}^{n-1}(q^n-q^i)}{q-1}$ – we can multiply a regular matrix by all non-zero elements of the field. We get $q-1$ different matrices. Exactly one of them has determinant 1, and so belongs to $SL_n(q)$.

(2) $Z(SL_n(q))$ consists of all diagonal matrices with all the entries on the diagonal equal (= scalar matrices) that belong to $SL_n(q)$. That is

$$\begin{pmatrix} a & 0 & 0 & \dots & 0 \\ 0 & a & 0 & \dots & 0 \\ 0 & 0 & a & \dots & 0 \\ & & \dots & & \\ 0 & 0 & 0 & \dots & a \end{pmatrix} \in Z(SL_n(q)) \quad \text{iff} \quad a^n = 1.$$

We have proved that the multiplicative group of a finite field of order q is cyclic of order $q-1$. The number of elements a from $\mathbb{Z}_{q-1}$ a cyclic group of order $q-1$ with $a^n = 1$ is $d = \gcd(n, q-1)$.
(For b from a cyclic group C of order $q-1$, $b^n = 1$ iff $b^{d = \gcd(n,q-1)} = 1$ iff b belongs to a unique subgroup of C of order d. This subgroup has exactly d-elements :)

We conclude that

$$|PSL_n(q)| = \frac{|SL_n(q)|}{|Z(SL_n(q))|} = \frac{\prod_{i=0}^{n-1}(q^n - q^i)}{d \cdot (q-1)}.$$

Example:

- $PSL_2(5) = \frac{(5^2-5)\cdot(5^2-1)}{2\cdot(5-1)} = \frac{20\cdot 24}{8} = 60$
- $PSL_2(4) = \frac{(4^2-4)(4^2-1)}{1\cdot(4-1)} = \frac{12\cdot 15}{3} = 60$

Theorem 7.6: $PSL_2(5) \simeq PSL_2(4) \simeq A_5$

Proof.

1) First we prove that $PSL_2(5) \simeq A_5$:

Let V be a two-dimensional vector space over the field $\mathbb{F}_5$. The vector space has exactly 6 one-dimensional subspaces (lines). They are multiples of the following vectors:

$$\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\2\end{pmatrix}, \begin{pmatrix}1\\3\end{pmatrix}, \begin{pmatrix}1\\4\end{pmatrix}$$

1 2 3 4 5 6

The group $SL_2(5)$ acts on the set of ~~the~~ lines:

$$\underset{\in SL_2(5)}{A} \cdot \underbrace{\{\alpha v \mid \alpha \in \mathbb{F}_5\}}_{\text{line}} = \{\alpha \cdot Av \mid \alpha \in \mathbb{F}_5\}.$$

Observe that $Z(SL_2(5)) = \left\{ \begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}4&0\\0&4\end{pmatrix} \right\}$. These are the only matrices which stabilises all the lines (i.e, the kernel of the action). The action of $SL_2(5)$ then induces an action of $PSL_2(5) = SL_2(5)/Z(SL_2(5))$, given by $\overline{A}\cdot \ell = A\ell$ where ℓ is a line, $A \in SL_2(5)$ and $\overline{A} = A\cdot Z(SL_2(5)) \in PSL_2(5)$.

Number the lines as above (red numbers). Consider matrices $A = \begin{pmatrix}1&0\\4&1\end{pmatrix}$ and $B = \begin{pmatrix}0&1\\4&1\end{pmatrix}$.

Put $C = \begin{pmatrix}0&1&1&1&1&1\\1&0&1&2&3&4\end{pmatrix}$, and compute

$$A\cdot C = \begin{pmatrix}1&0\\4&1\end{pmatrix}\underset{1\ 2\ 3\ 4\ 5\ 6}{\begin{pmatrix}0&1&1&1&1&1\\1&0&1&2&3&4\end{pmatrix}} = \underset{1\ 6\ 2\ 3\ 4\ 5}{\begin{pmatrix}0&1&1&1&1&1\\1&4&0&1&2&3\end{pmatrix}}$$

$$B\cdot C = \begin{pmatrix}0&1\\4&1\end{pmatrix}\underset{1\ 2\ 3\ 4\ 5\ 6}{\begin{pmatrix}0&1&1&1&1&1\\1&0&1&2&3&4\end{pmatrix}} = \underset{3\ 1\ 2\ 5\ 6\ 4}{\begin{pmatrix}1&0&1&2&3&4\\1&4&0&1&2&3\end{pmatrix}}$$

Note that $\underbrace{\langle\begin{pmatrix}0\\4\end{pmatrix}\rangle}_{\text{the subspace generated by } \binom{0}{4}} = \underbrace{\langle\begin{pmatrix}1\\0\end{pmatrix}\rangle}_{\text{the subspace generated by } \binom{1}{0}}, \langle\begin{pmatrix}2\\1\end{pmatrix}\rangle = \langle\begin{pmatrix}1\\3\end{pmatrix}\rangle, \langle\begin{pmatrix}3\\2\end{pmatrix}\rangle = \langle\begin{pmatrix}1\\4\end{pmatrix}\rangle$ and $\langle\begin{pmatrix}4\\3\end{pmatrix}\rangle = \langle\begin{pmatrix}1\\2\end{pmatrix}\rangle$.

... etc

The action of $SL_2(5)$ and the numbering of lines gives us a homomorphism

$$SL_2(5) \longrightarrow S_6 .$$

with kernel $Z(SL_2(5))$. This induces an one-to-one homomorphism $PSL_2(5) \to S_6$. Its image is isomorphic to $PSL_2(5)$. We know that the image contains a subgroup generating by permutations $(2\,3\,4\,5\,6)$ (multiplication by A) and $(1\,2\,3)(4\,6\,5)$ (multiplication by B). From the study of rotations of a icosahedron, we know that these two permutations ~~induces~~ generates a subgroup of S_6 isomorphic to A_5. Comparing the orders, we get that $60 = |PSL_2(5)| = |A_5|$ and so this subgroup is the image of the action. Hence $PSL_2(5) \simeq A_5$.

b) Now we prove that $PSL_2(4) \simeq A_5$.

- First we investigate the ~~multi~~ 4 element field $GF(4)$. It can be constructed as a splitting field of the polynomial x^2+x+1 (which is irreducible as it has no root and it has a degree 2) over the field $\mathbb{Z}_2$. Its elements can be identified with polynomials of degree ≤ 1, when multiblication is computed modulo the polynomial x^2+x+1. Therefore the elements are $0, 1, x, y = x+1$ and the operations are

+	0	1	x	y
0	0	1	x	y
1	1	0	y	x
x	x	y	0	1
y	y	x	1	0

·	0	1	x	y
0	0	0	0	0
1	0	1	x	y
x	0	x	y	1
y	0	y	1	x

- Note that
  - $x \cdot x = x^2 \equiv x+1 = y \pmod{x^2+x+1}$, $xy = yx = x^2+x \equiv 1 \pmod{x^2+x+1}$ and $y^2 = x^2+1 \equiv x \pmod{x^2+x+1}$.

There are five lines in the 2-dimensional vector space over the field $GF(4)$. Namely

$$\begin{pmatrix}0\\1\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\1\end{pmatrix}, \begin{pmatrix}1\\x\end{pmatrix}, \begin{pmatrix}1\\y\end{pmatrix}$$

1 2 3 4 5

As above we have an action of $SL_2(4)$ on the set of lines with the kernel $Z(SL_2(4))$ of scalar matrices (in fact in our case the kernel is trivial). This induces an one-to-one homomorphism $\psi: PSL_2(4) \to S_5$.

Consider matrices $A = \begin{pmatrix} x & y \\ x & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Note that $\det A = -xy = -1 = 1$ and $\det B = -1 = 1$ (as we compute in $GF(4)$), therefore $A, B \in SL_2(4)$. Put $C = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & x & y \end{pmatrix}$ and compute

$$AC = \begin{pmatrix} x & y \\ x & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & x & y \\ \scriptstyle 1 & \scriptstyle 2 & \scriptstyle 3 & \scriptstyle 4 & \scriptstyle 5 \end{pmatrix} = \begin{pmatrix} y & x & 1 & y & 0 \\ 0 & x & x & x & x \\ \scriptstyle 2 & \scriptstyle 3 & \scriptstyle 4 & \scriptstyle 5 & \scriptstyle 1 \end{pmatrix}$$

$$BC = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & x & y \\ \scriptstyle 1 & \scriptstyle 2 & \scriptstyle 3 & \scriptstyle 4 & \scriptstyle 5 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & y & x \\ 0 & 1 & 1 & 1 & 1 \\ \scriptstyle 2 & \scriptstyle 3 & \scriptstyle 1 & \scriptstyle 4 & \scriptstyle 5 \end{pmatrix}$$

Since $\langle \binom{y}{0} \rangle = \langle \binom{1}{0} \rangle$, $\langle \binom{x}{x} \rangle = \langle \binom{1}{1} \rangle$, $\langle \binom{y}{x} \rangle = \langle \binom{1}{y} \rangle$, and $\langle \binom{0}{x} \rangle = \langle \binom{0}{1} \rangle$, the multiplication by $\bar{A}$ (and so by $\bar{A}$) corresponds to the permutation (54321).

Since $\langle \binom{y}{1} \rangle = \langle \binom{1}{x} \rangle$ and $\langle \binom{x}{1} \rangle = \langle \binom{1}{y} \rangle$, multiplication by B (resp. by $\bar{B}$) corresponds to (132).

- We leave as an exercise that the permutations (54321) and (132) generate A_5.

Since $|PSL_2(4)| = 60 = |A_5|$, A_5 is the image of ψ and since ψ is one-to-one, $A_5 \simeq PSL_2(4)$. □

Exercise: Prove that $PSL_2(2) \simeq S_3$ and $PSL_2(3) \simeq A_4$.

Recall: A group G acts

- ~~faithfully~~ on a set X <u>faithfully</u> if for every $g \neq 1$ in G, there is $x \in X$ with $g \cdot x \neq x$.
- on a set X <u>2-transitively</u> if for any $x_1 \neq x_2$ and $y_1 \neq y_2$ in X, there is $g \in G$ with $g \cdot x_1 = y_1$ and $g \cdot x_2 = y_2$.

Leonard Eugene Dickson
1874 – 1954

Lemma 7.7.: Suppose that a group G acts faithfully and 2-transitively on a set X. Moreover, assume that

1) $G = [G,G]$;

2) for every $x \in X$, there is an abelian normal subgroup A of $St_G(x)$ with $G = \langle \bigcup_{g \in G} gAg^{-1} \rangle$.

Then G is simple.

Proof: Let N be a non-trivial normal subgroup of G.

Recall Proposition 2.12. If a group G acts faithfully and 2-transitively on a set X, then every non-trivial normal subgroup of G acts on X transitively. $\perp$

It follows that N acts transitively on X, hence $G = N \cdot St_G(x)$ for every $x \in X$.

Claim 1. $G = NA$.

Proof of Claim 1. Since $G = \langle \bigcup_{g \in G} gAg^{-1} \rangle$, every $g \in G$ is of the form

$$g = g_1 a_1 g_1^{-1} \, g_2 a_2 g_2^{-1} \, g_3 a_3 g_3^{-1} \cdots g_k a_k g_k^{-1}$$

for some $g_i \in G$ and $a_i \in A$, $i = 1, \dots, k$.

Since $G = N \cdot St_G(x)$, for every $i = 1, \dots, k$, $g_i = n_i s_i$ with $n_i \in N$ and $s_i \in St_G(x)$.

Since $N \trianglelefteq G$,

$$g \cdot N = s_1 a_1 s_1^{-1} \, s_2 a_2 s_2^{-1} \cdots s_k a_k s_k^{-1} \cdot N,$$

and since $A \trianglelefteq St_G(x)$,

$$s_1 a_1 s_1^{-1} \cdots s_k a_k s_k^{-1} \in A$$

Therefore $g \in A \cdot N = N \cdot A$. $\perp$

Since A is an abelian group and $NA/N \simeq A/N\cap A$, we have that $[NA, NA] \leq N$.

From $G = [G,G]$ (one of the assumptions) and $G = NA$, we get that

$$N \leq G = [G,G] = [NA, NA] \leq N,$$

hence $N = G$. □

TRANSVECTIOS :

- For $1 \leq k, l \leq n$, let E_{kl} be the matrix with only non-zero entry 1 in the intersection of the k^{th} row and the l^{th} column. Formaly, $E_{kl} = (e_{ij})$, where

$$e_{ij} = \begin{cases} 1 & : i = k, j = l, \\ 0 & : \text{otherwise}. \end{cases}$$

- $E = \sum_{i=1}^{n} E_{ii}$ is the diagonal (unit) matrix.

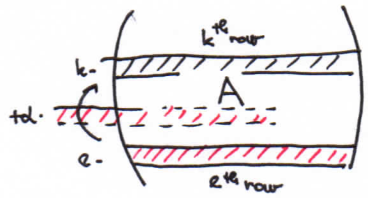
- $E_{ij} E_{kl} = \begin{cases} E_{il} & \text{if } j = k \\ 0 & \text{otherwise}. \end{cases}$

- Let $\alpha \in \mathbb{E}$ and $k \neq l$ be from $\{1, \dots, n\}$. The corresponding elementary transvection is the matrix

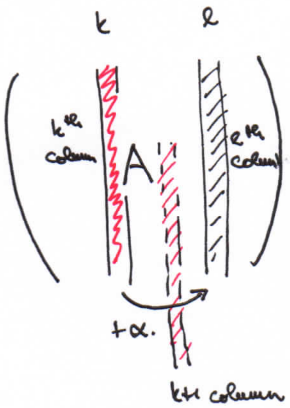
  - $T_{kl}(\alpha) = E + \alpha E_{kl}$

  - $T_{kl}(\alpha)^{-1} = T_{kl}(-\alpha)$

  - Multiplying a matrix A by $T_{kl}(\alpha)$ from the left results in adding α^{th} multiple of l^{th} row of A to k^{th} row.

$T_{kl}(\alpha) A =$ 

  - Multiplying a matrix A by $T_{kl}(\alpha)$ from the right results in adding the α^{th}-multiple of the k^{th} column of A to the l^{th} column of A



Lemma 7.8: Let $\mathbb{F}$ be a field, let $A \in GL_n(\mathbb{F})$. Then

$$A = T \cdot D(\underline{\mu}),$$

where T is a product of elementary transvections and $D = \operatorname{diag}\{1, 1, \dots, 1, \mu\}$ is the diagonal matrix with $\underline{\mu} = \langle 1, 1, \dots, 1, \mu \rangle$ on the diagonal.

Proof:

- It suffices to prove that A can be transformed by elementary transformations "add some multiple of a row to another different row" to the matrix $D(\underline{\mu})$.
- Since A is regular, the first column of A is non-zero. By adding a suitable multiple of a j-th row with $a_{j1} \neq 0$ to the second row, we can get $a_{21} \neq 0$. Then by adding $\frac{1 - a_{11}}{a_{21}}$ multipl of the second row to the first one (i.e, by multiplying by the transvection $T_{12}\left(\frac{1-a_{11}}{a_{21}}\right)$ on the left, we get $a_{11} = 1$. Having this, we can make first entries of other rows 0. We get the matrix

$$A_1 = \begin{pmatrix} 1 & \\ 0 & \\ \vdots & B_1 \\ 0 & \end{pmatrix};$$

where B_1 is some $n \times (n-1)$ matrix and $\det A_1 = \det A_1 \neq 0$. (determinant of all transvections is 1, therefore multiplying by it does not change the determinant).

- Suppose that we have transformed the matrix A to the matrix A_j of the form

$$A_j = \begin{pmatrix} E_j & B_j \\ 0 & \end{pmatrix},$$

where E_j denotes the unit $j \times j$ matrix and B_j is some $n \times (n-j)$ matrix, with $\det A_j = \det A \neq 0$. Let

$$B_j = \begin{pmatrix} D_j \\ C_j \end{pmatrix}$$

where C_j is a $(n-j) \times (n-j)$ matrix. Since $0 \neq \operatorname{Det} A_j = \operatorname{Det} C_j$, C_j is regular. As in the first step of our construction, we can by a series of transvections transform the matrix C_j to $C_j' = \begin{pmatrix} 1 & \\ 0 & \\ \vdots & C_j'' \\ 0 & \end{pmatrix}$ and then by adding suitable multiples of the $(j+1)^{th}$ row to $j^{th}, (j-1)^{th}, \dots, 1^{st}$ row, we obtain a matrix

$$A_{j+1} = \begin{pmatrix} E_{j+1} & D_{j+1} \\ 0 & \end{pmatrix}$$

where B_{j+1} is some $n \times (n-(j+1))$ matrix. Moreover, $\det A_{j+1} = \det A$.

- Arguing by induction, we can transform A to the matrix

$$A_{n-1} = \begin{pmatrix} E_{n-1} & C_{n-1} \\ 0 & \mu \end{pmatrix},$$

where $\mu = \det A_{n-1} = \det A$. By adding suitable multiples of the ~~first~~ last row to other rows, we get the matrix $D(\underline{\mu})$. ∎

Corollary 7.9.: The group $SL_n(\mathbb{F})$ is generated by transvections.

- For $\underline{c} = \langle c_1, c_2, \dots, c_n \rangle$ let $D(\underline{c}) = \mathrm{diag}\langle c_1, \dots, c_n \rangle$ denote the matrix

$$D(\underline{c}) = \begin{pmatrix} c_1 & 0 & 0 & \dots & 0 \\ 0 & c_2 & 0 & \dots & 0 \\ 0 & 0 & c_3 & \dots & 0 \\ & & \dots & & \\ 0 & 0 & 0 & \dots & c_n \end{pmatrix} = \sum_{i=1}^{n} c_i E_{ii}$$

$\triangleleft$ Put $\underline{c}^{-1} = \langle c_1^{-1}, \dots, c_n^{-1} \rangle$ and observe that $D(\underline{c})^{-1} = D(\underline{c}^{-1})$.

Lemma 7.10.:

1. Let i, j, k be distinct. Then

$$[T_{ij}(\alpha), T_{jk}(\beta)] = T_{ik}(\alpha\beta)$$

2. Let $1 \le i \ne j \le n$, $\underline{c} = \langle c_1, \dots, c_n \rangle$ ($c_i \ne 0$ for all $i = 1, \dots, n$). Then

$$[T_{ij}(\alpha), D(\underline{c})] = T_{ij}\left(\alpha \cdot \left(1 - \frac{c_i}{c_j}\right)\right)$$

Proof:

1. $$[T_{ij}(\alpha), T_{jk}(\beta)] = T_{ij}(\alpha) T_{jk}(\beta) T_{ij}(-\alpha) T_{jk}(-\beta) = (E + \alpha E_{ij})(E + \beta E_{jk})(E - \alpha E_{ij})(E - \beta E_{jk})$$
$$= (E + \alpha E_{ij} + \beta E_{jk} + \alpha\beta E_{ik})(E - \alpha E_{ij} - \beta E_{jk} + \alpha\beta E_{ik}) =$$
$$= E + \alpha E_{ij} + \beta E_{jk} + \alpha\beta E_{ik} - \alpha E_{ij} - \beta E_{jk} - \alpha\beta E_{ik} + \alpha\beta E_{ik} = E + \alpha\beta E_{ik} = T_{ik}(\alpha\beta)$$

2. $$[T_{ij}(\alpha), D(\underline{c})] = T_{ij}(\alpha) D(\underline{c}) T_{ij}(-\alpha) D(\underline{c}^{-1}) = (E + \alpha E_{ij})\left(\sum_{i=1}^{n} c_i E_{ii}\right)(E - \alpha E_{ij})\left(\sum_{i=1}^{n} \frac{1}{c_i} E_{ii}\right)$$
$$= \left(\sum_{i=1}^{n} c_i E_{ii} + \alpha c_j E_{ij}\right)\left(\sum_{i=1}^{n} \frac{1}{c_i} E_{ii} - \alpha \frac{1}{c_j} E_{ij}\right)$$
$$= E - \alpha \frac{c_i}{c_j} E_{ij} + \alpha E_{ij} = E + \alpha\left(1 - \frac{c_i}{c_j}\right) E_{ij} = T_{ij}\left(\alpha\left(1 - \frac{c_i}{c_j}\right)\right).$$

$\square$

- For a permutation $\sigma \in S_n$ put

$$P_\sigma = \sum_{i=1}^{n} E_{\sigma(i) i}$$

$\triangleleft$ $P_\sigma P_\tau = P_{\sigma\tau}$ for all $\sigma, \tau \in S_n$.

Lemma 7.11: Let $i \ne j$, $\alpha \in \mathbb{F}$ and $\sigma \in S_n$. Then

$$P_\sigma T_{ij}(\alpha) P_\sigma^{-1} = T_{\sigma(i)\sigma(j)}(\alpha).$$

Proof.
$$P_\sigma T_{ij}(\alpha) P_\sigma^{-1} = \left(\sum_{i=1}^{n} E_{\sigma(i) i}\right)(E + \alpha E_{ij})\left(\sum_{i=1}^{n} E_{i\sigma(i)}\right) =$$
$$= E + \alpha\left(\sum_{i=1}^{n} E_{\sigma(i) i}\right) E_{ij} \left(\sum_{i=1}^{n} E_{i\sigma(i)}\right) =$$
$$= E + \alpha \cdot E_{\sigma(i) i} E_{ij} E_{j\sigma(j)} = E + \alpha E_{\sigma(i)\sigma(j)} = T_{\sigma(i)\sigma(j)}(\alpha).$$

$\square$

Theorem (Jordan-Dickson): Let $n \geq 2$ and q be a power of a prime p.

7.13 The group $PSL_n(q)$ is simple with two exceptions:

$PSL_2(2) \simeq S_3$ and $PSL_2(3) \simeq A_4$.

Proof: Let $\mathbb{F}$ be a q-element field, let $V = \mathbb{F}^n$ be a vector space over $\mathbb{F}$, let $e_1, \dots, e_n$ be the standard basis of $\mathbb{F}$. Let X denote the set of lines of V. For a non-zero vector $v \in V$ denote by $\bar{v}$ the line containging (determined by v).

Let $SL_n(q)$ act on X by $A\bar{v} = \overline{Av}$. For a non-zero $v \in V$ and $0 \neq \lambda \in \mathbb{F}$ $\overline{Av} = \overline{\lambda Av} = \overline{A\lambda v}$, therefore the action is well defined. One easily verifies that $AB\bar{v} = A\overline{Bv}$ and that $E\bar{v} = \bar{v}$ for the identity matrix E.

Claim 1: The kernel of the action of $SL_n(q)$ on X is $Z(SL_n(q))$.

Proof of Claim 1: $Av = \lambda v$ for every vector v iff A is a scalar matrix. $Z(SL_n(q))$ consists of all scalar matrices from $SL_n(q)$. $\perp$

- For a matrix $A \in SL_n(q)$ let $\bar{A}$ denote the corresponding element from $PSL_n(q)$.

It follows from Claim 1 that defining $\bar{A}\bar{v} = \overline{Av}$, we get a faithful action of $PSL_n(q)$ on X. We verify that this action satisfies all properties of Lemma 7.7.

Claim 2: The action of $PSL_n(q)$ on X is 2-transitive.

Proof of Claim 2: Let $\overline{v_1} \neq \overline{v_2}$ be a pair of distinct lines from X. Let A be a regular matrix of the form $(v_1|v_2|\dots)$, that is, a regular matrix with vectors v_1 and v_2 in the first two columns. But $B = \frac{1}{\det A} \cdot A \in SL_n(q)$. Then $Be_1 = v_1$ and $Be_2 = v_2$, hence $\bar{B}\,\bar{e}_1 = \bar{v}_1$ and $\bar{B}\,\bar{e}_2 = \bar{v}_2$. This implies 2-transitivity of the action. $\perp$

Claim 3: $PSL_n(q) = [PSL_n(q), PSL_n(q)]$.

Proof of Claim 3: Readily from the definition of commutator one gets that

$$[PSL_n(q), PSL_n(q)] = \left[{}^{SL_n(q)}\!/_{Z(SL_n(q))}, {}^{SL_n(q)}\!/_{Z(SL_n(q))} \right] = {}^{[SL_n(q), SL_n(q)]}\!/_{Z(SL_n(q))}$$

Therefor it suffices to show that

$$SL_n(q) = [SL_n(q), SL_n(q)].$$

Clearly $[SL_n(q), SL_n(q)] \subseteq SL_n(q)$. For the opposite inclusion, it will suffice to prove that $[SL_n(q), SL_n(q)]$ contains all transvections.

This follows from Lemma 7.10 (1) in case $n \geq 3$.

Observe that if $q > 3$, then the field $\mathbb{F}$ contains $a \neq 0$ such that $a = a^{-1}$ (indeed, the polynomial x^2+1 has at most two roots and we have at least 3 non-zero elements of $\mathbb{F}$). Then $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ is a diagonal non-scalar matrix in $SL_2(q)$. Applying Lemma 7.10 (2), we get that $[SL_2(q), SL_2(q)]$ contains all transvections as well. $\perp$

Let $x := \overline{e_n}$. Then

$$St_{PSL_n(q)}(x) = \{ \overline{B} \mid B \in SL_n(q) \text{ and } b_{1n} = b_{2n} = \dots = b_{n-1\,n} = 0 \}.$$

Thus the stabilizer of x consists of images $\overline{B}$ of matrices of the form

$$B = \left(\begin{array}{ccc|c} & B' & & 0 \\ \hline b_{n1} & \dots & b_{nn-1} & b_{nn} \end{array}\right) = \sum_{i=1}^{n} \sum_{j=1}^{n-1} b_{ij} E_{ij} + b_{nn} E_n$$

with $\det B = 1$.

Observe that

$$B^{-1} = \left(\begin{array}{ccc|c} & B'^{-1} & & 0 \\ \hline b'_{n1} & \dots & b'_{nn-1} & b'_{nn} \end{array}\right) = \sum_{i=1}^{n} \sum_{j=1}^{n-1} b'_{ij} E_{ij} + b'_{nn} E_n \text{, with } b'_{ij} \text{ suitable elements of } \mathbb{F} \text{ and } b'_{nn} = b_{nn}^{-1}.$$

- Put $\mathcal{A} = \{ \overline{E + \sum_{j=1}^{n-1} a_{nj} E_{nj}} \mid a_{nj} \in \mathbb{F} \text{ for } j = 1, \dots, n-1 \}$

Elements of $\mathcal{A}$ are matrices of the form

$$\left(\begin{array}{ccc|c} & E & & 0 \\ \hline a_{n1} & \dots & a_{nn-1} & 1 \end{array}\right).$$

Claim 4: $\mathcal{A}$ is an abelian normal subgroup of $St_{PSL_n(q)}(x)$.

Proof of claim 4: Clearly $\mathcal{A} \subseteq St_{PSL_n(q)}(x)$.

Let $\overline{A} = \overline{E + \sum_{j=1}^{n-1} a_{nj} E_{nj}}$ and $\overline{B} = \overline{E + \sum_{j=1}^{n-1} b_{nj} E_{nj}}$ be two matrices from $\mathcal{A}$. Then

$$\overline{A}\,\overline{B} = \overline{(E + \sum_{j=1}^{n-1} a_{nj} E_{nj})(E + \sum_{j=1}^{n-1} b_{nj} E_{nj})} = \overline{E + \sum_{j=1}^{n-1} (a_{nj} + b_{nj}) E_{nj}} \in \mathcal{A}$$

and

$$\overline{B}\,\overline{A} = \overline{E + \sum_{j=1}^{n-1} (b_{nj} + a_{nj}) E_{nj}} = \overline{E + \sum_{j=1}^{n-1} (a_{nj} + b_{nj}) E_{nj}} = \overline{A}\,\overline{B}.$$

Therefore $\mathcal{A}$ is an abelian subgroup of $St_{PSL_n(q)}(x)$.

Let $A = E + \sum_{j=1}^{m-1} a_{mj} E_{mj}$ and $B = \sum_{i=1}^{m}\sum_{j=1}^{m-1} b_{ij} E_{ij} + b_{mm} E_{mm}$ be matrices with $\bar{A} \in \mathcal{A}$ and $\bar{B} \in St_{SPL_m(q)}(X)$. Let b'_{ij} be such that $B^{-1} = \sum_{i=1}^{m}\sum_{j=1}^{m-1} b'_{ij} E_{ij} + b'_{mm} E_{mm}$.

We compute that

$$BAB^{-1} = B\Big(E + \sum_{j=1}^{m-1} a_{mj} E_{mj}\Big)B^{-1} = E + B\Big(\sum_{j=1}^{m-1} a_{mj} E_{mj}\Big)B^{-1} =$$

$$= E + \Big(\sum_{i=1}^{m}\sum_{j=1}^{m-1} b_{ij} E_{ij} + b_{mm} E_{mm}\Big)\Big(\sum_{j=1}^{m-1} a_{mj} E_{mj}\Big)\Big(\sum_{i=1}^{m}\sum_{j=1}^{m-1} b'_{ij} E_{ij} + b'_{mm} E_{mm}\Big) =$$

$$= E + \sum_{k=1}^{m-1} b_{mm} \underbrace{\Big(\sum_{j=1}^{m-1} a_{mj} b'_{jk}\Big)}_{a'_{mk}} E_{mk} = E + \sum_{k=1}^{m-1} a'_{mk} E_{mk}.$$

Therefore $\overline{BAB^{-1}} \in \mathcal{A}$.

We conclude that $\mathcal{A} \trianglelefteq St_{PSL_m(q)}(X)$.

Claim 5. The group G generated by all $\overline{CAC^{-1}}$, $\bar{C} \in PSL_m(q)$, $\bar{A} \in \mathcal{A}$ is equal to $PSL_m(q)$.

Proof of Claim 5.

Since the group $SL_m(q)$ is generated by transvections, due to Lemma 7.8 (Corollary 7.9), it suffices to prove that the group generated by matrices CAC^{-1}, where $\bar{A} \in \mathcal{A}$ and $C \in SL_n(q)$ contains all transvections. Let $1 \le i \ne j \le n$, $\alpha \in \mathbb{F} \setminus \{0\}$. We show that the group contains the tranvection $T_{ij}(\alpha)$. Note that $\overline{T_{m1}(\alpha)} \in \mathcal{A}$ for all $\alpha \in \mathbb{F} \setminus \{0\}$.

Pick a permutation σ such that $\sigma(m) = i$ and $\sigma(1) = j$. If σ is even or char $\mathbb{F} = 2$, det $P_\sigma = 1$, and so $P_\sigma \in SL_m(q)$. Applying Lemma 11, we get that

$$P_\sigma T_{n1}(\alpha) P_\sigma^{-1} = T_{\sigma(n)\sigma(1)}(\alpha) = T_{ij}(\alpha).$$

Suppose that char $\mathbb{F} \ne 2$ and σ is odd. Let $D := E - 2E_{11}$ be the diagonal matrix $\begin{pmatrix} -1 & 0 & 0 & \cdots \\ 0 & 1 & 0 & \cdots \\ 0 & 0 & 1 & \cdots \\ 0 & 0 & 0 & \ddots & 1 \end{pmatrix}$. Note that $D^2 = E$, hence $D = D^{-1}$ and $P_\sigma D \in SL_m(q)$ (indeed, $\det P_\sigma D = \det P_\sigma \det D = (-1)^2$).

We compute that

$$P_\sigma D T_{m1}(\alpha) (P_\sigma D)^{-1} = P_\sigma D T_{m1}(-\alpha) D P_\sigma^{-1} = P_\sigma (E - 2E_{11})(E - \alpha E_{m1})(E - 2E_{11}) P_\sigma^{-1}$$

$$= P_\sigma (E + \alpha E_{m1}) P_\sigma^{-1} = P_\sigma T_{m1}(\alpha) P_\sigma^{-1} = T_{ij}(\alpha)$$

(as above, using Lemma 11.)

Now application of Lemma 7.7 concludes the proof. □